==Phrack Inc.==

Volume Two, Issue Eleven, Phile #1 of 12

Index

2/17/87

Welcome to Issue Eleven of the Phrack Inc. electronic newsletter. This issue, I was a bit more reliable about getting the issue out (yes, only 3 days late!). This issue did not come together as easily as I would have hoped due to a number of people being difficult to get a hold of or getting their files, but I filled their places in with other files, so if you had been told you would have a file in this issue, get in contact with me so that it will be featured in Issue Twelve. The following files are featured in this edition of Phrack Inc.:

Taran King
Sysop of Metal Shop Private

==Phrack Inc.==

Volume Two, Issue Eleven, Phile #10 of 12

BUSY LINE VERIFICATION

WRITTEN BY PHANTOM PHREAKER

This file describes how a TSPS operator does a BLV (Busy Line Verification) and an EMER INT (Emergency Interrupt) upon a busy line that a customer has requested to be 'broken' into. I have written this file to hopefully clear up all the misconceptions about Busy Line Verification and Emergency Interrupts.

BLV is 'Busy Line Verification'. That is, discovering if a line is busy/not busy. BLV is the telco term, but it has been called Verification, Autoverify, Emergency Interrupt, break into a line, REMOB, and others. BLV is the result of a TSPS that uses a Stored Program Control System (SPCS) called the Generic 9 program. Before the rise of TSPS in 1969, cordboard operators did the verification process. The introduction of BLV via TSPS brought about more operator security features. The Generic 9 SPCS and hardware was first installed in Tucson, Daytona, and Columbus, Ohio, in 1979. By now virtually every TSPS has the Generic 9 program.

A TSPS operator does the actual verification. If caller A was in the 815 Area code, and caller B was in the 314 Area code, A would dial 0 to reach a TSPS in his area code, 815. Now, A, the customer, would tell the operator he wished an emergency interrupt on B's number, 314+555+1000. The 815 TSPS op who answered A's call cannot do the interrupt outside of her own area code, (her service area), so she would call an Inward Operator for B's area code, 314, with KP+314+TTC+121+ST, where the TTC is a Terminating Toll Center code that is needed in some areas. Now a TSPS operator in the 314 area code would be reached by the 815 TSPS, but a lamp on the particular operators console would tell her she was being reached with an Inward routing. The 815 operator then would say something along the lines of she needed an interrupt on 314+555+1000, and her customers name was J. Smith. Now, the 314 Inward (which is really a TSPS) would dial B's number, in a normal Operator Direct Distance Dialing (ODDD) fashion. If the line wasn't busy, then the 314 Inward would report this to the 815 TSPS, who would then report to the customer (caller A) that 314+555+1000 wasn't busy and he could call as normal. However if the given number (in this case, 314+555+1000) was busy, then several things would happen and the process of BLV and EMER INT would begin. The 314 Inward would seize a Verification trunk (or BLV trunk) to the toll office that served the local loop of the requested number (555+1000). Now another feature of TSPS checks the line asked to be verified against a list of lines that can't be verified, such as radio stations, police, etc. If the line number a customer gives is on the list then the verification cannot be done, and the operator tells the customer.

Now the TSPS operator would press her VFY (VeriFY) key on the TSPS console, and the equipment would outpulse (onto the BLV trunk) KP+0XX+PRE+SUFF+ST. The KP being Key Pulse, the 0XX being a 'screening code' that protects against trunk mismatching, the PRE being the Prefix of the requested number (555), the SUFF being the Suffix of the requested number (1000), and the ST being STart, which tells the Verification trunk that no more MF digits follow. The screening code is there to keep a normal Toll Network (used in regular calls) trunk from accidentally connecting to a Verification trunk. If this screening code wasn't present, and a trunk mismatch did occur, someone calling a friend in the same area code might just happen to be connected to his friends line, and find himself in the middle of a conversation. But, the Verification trunk is waiting for an 0XX sequence, and a normal call on a Toll Network trunk does not outpulse an 0XX first. (Example: You live at 914+555+1000, and wish to call 914+666+0000. The routing for your call would be KP+666+0000+ST. The BLV trunk cannot accept a 666 in place of the proper 0XX routing, and thus would give the caller a re-order tone.) Also, note that the outpulsing sequence onto a BLV trunk can't contain an Area Code. This is the reason why if a customer requests an interrupt outside of his own NPA, the TSPS operator must call an Inward for the area code that can outpulse onto the proper trunk. If a TSPS in 815 tried to do an

interrupt on a trunk in 314, it would not work. This proves that there is a BLV network for each NPA, and if you somehow gain access to a BLV trunk, you could only use it for interrupts within the NPA that the trunk was located in.

BLV trunks 'hunt' to find the right trunks to the right Class 5 End Office that serves the given local loop. The same outpulsing sequence is passed along BLV trunks until the BLV trunk serving the Toll Office that serves the given End Office is found.

There is usually one BLV trunk per 10,000 lines (exchange). So, if a Toll Office served ten End Offices, that Toll Office would have 100,000 local loops that it served, and have 10 BLV trunks running from TSPS to that Toll Office.

Now, the operator (in using the VFY key) can hear what is going on on the line, (modem, voice, or a permanent signal, indicating a phone off-hook) and take appropriate action. She can't hear what's taking place on the line clearly, however. A speech scrambler circuit within the operator console generates a scramble on the line while the operator is doing a VFY. The scramble is there to keep operators from listening in on people, but it is not enough to keep an op from being able to tell if a conversation, modem signal, or a dial tone is present upon the line. If the operator hears a permanent signal, she can only report back to the customer that either the phone is off-hook, or there is a problem with the line, and she can't do anything about it. In the case of caller A and B, the 314 Inward would tell the 815 TSPS, and the 815 TSPS would tell the customer. If there is a conversation on line, the operator presses a key marked EMER INT (EMERgency INTerrupt) on her console. This causes the operator to be added into a three way port on the busy line. The EMER INT key also deactivates the speech scrambling circuit and activates an alerting tone that can be heard by the called customer. The alerting tone that is played every 10 seconds tells the customer that an operator is on the line. Some areas don't have the alerting tone, however. Now, the operator would say 'Is this XXX-XXXX?' where XXX-XXXX would be the Prefix and Suffix of the number that the original customer requesting the interrupt gave the original TSPS. The customer would confirm the operator had the correct line. Then the Op says 'You have a call waiting from (customers name). Will you accept?'. This gives the customer the chance to say 'Yes' and let the calling party be connected to him, while the previous party would be disconnected. If the customer says 'No', then the operator tells the person who requested the interrupt that the called customer would not accept. The operator can just inform the busy party that someone needed to contact him or her, and have the people hang up, and then notify the requesting customer that the line is free. Or, the operator can connect the calling party and the interrupted party without loss of connection.

The charges for this service (in my area at least) run 1.00 for asking the operator to interrupt a phone call so you can get through. There is an .80 charge if you ask the operator to verify whether the phone you're trying to reach is busy because of a service problem or because of a conversation. If the line has no conversation on it, there will be no charge for the verification.

When the customer who initiated the emergency interrupt gets his telephone bill, the charges for the interrupt call will look similar to this:

```
12-1   530P     INTERRUPT  CL       314 555 1000  OD     1                1.00
```

The 12-1 is December first of the current year; 530P is the time the call was made to the operator requesting an interrupt; INTERRUPT CL is what took place, that is, an interrupt call; 314 555 1000 is the number requested; OD stands for Operator Dialed; the 1 is the length of the call (in minutes); and the 1.00 is the charge for the interrupt. The format may be different, depending upon your area and telephone company.

One thing I forgot to mention about TSPS operators. In places where a Remote Trunking Arrangement is being used, and even places where they aren't in use, you may be connected to a TSPS operator in a totally different area code. In such a case, the TSPS that you reach in a Foreign NPA will call up an inward operator for your Home NPA, if the line you requested an EMER INT on was in your HNPA. If the line you requested EMER INT on was in the same NPA of the TSPS that you had reached, then no inward operator would be needed and the

answering operator could do the entire process.

Verification trunks seem to be only accessible by a TSPS/Inward operator. However, there have been claims to people doing Emergency Interrupts with blue boxes. I don't know how to accomplish an EMER INT without the assistance of an operator, and I don't know if it can be done. If you really wish to participate in a BLV/EMER INT, call up an Inward Operator and play the part of a TSPS operator who needs an EMER INT upon a pre-designated busy line. Billing is handled at the local TSPS so you will not have to supply a billing number if you decide to do this.

If you find any errors in this file, please try to let me know about it, and if you find out any other information that I haven't included, feel free to comment.

-End of file-

==Phrack Inc.==

Volume Two, Issue Eleven, Phile #11 of 12

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                                     PWN
PWN                      *>=-{ Phrack World News }-=<*                  PWN
PWN                                                                     PWN
PWN                                 Issue X                             PWN
PWN                                                                     PWN
PWN                      Written, Compiled, and Edited                  PWN
PWN                           by Knight Lightning                       PWN
PWN                                                                     PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Scan Man Revisited — January 19, 1987

The following is a reprint from TeleComputist Newsletter Issue Two;

SCAN MAN - FED OR PHREAK? (The Other Side)

TeleComputist is printing the statement Scan Man has made to us [TeleComputist] in rebuttal to Phrack World News, whom previously printed an article concerning Scan Man in Phrack Issue VIII. Those of you who have seen or read the article in Phrack VIII know that it basically covered information and an intercepted memo alleging Scan Man of going after hackers and turning in codes off his BBS (P-80 Systems, Charleston, West Virginia 304/744-2253) as a TMC employee. Please note that this statement should be read with the article concerning Scan Man in Phrack Issue VIII to get the full understanding.

Scan Man started off his statement claiming not to work for TMC, but instead for a New York branch office of Telecom Management (a Miami based firm). He was flown in from Charleston, West Virginia to New York every week for a four to five day duration. Once in New York, Telecom Management made available a leased executive apartment where Scan Man stayed as he worked. His position in Telecom Management was that of a systems analyst, "...and that was it!" Scan Man stated. Scan Man also stated that he had never made it a secret that he was working in New York and had even left messages on his BBS saying this.

He also went on to say that he had no part in the arrest of Shawn [of Phreaker's Quest] (previously known as Captain Caveman) by TMC in Las Vegas. Scan Man claimed to have no ties with TMC in Las Vegas and that they would not even know him. Scan Man then went on to say that Shawn had never replied to previous messages Scan man had left asking for TMC codes. Scan Man also said that the messages about TMC were in no way related to him. He claimed to have no ties to TMC, which is a franchised operation which makes even TMC unrelated except by name.

Scan Man stated that he called Pauline Frazier and asked her about the inquiry by Sally Ride [:::Space Cadet] who acted as an insider to obtain the information in Phrack VIII. He said that Pauline said nothing to the imposter (Sally Ride) and merely directed him to a TMC employee named Kevin Griffo. Scan Man then went on to say that the same day Sally Ride called Pauline Frazier was the same day he received his notice. And to that Scan Man made the comment, "If I find out this is so heads will roll!"

After that comment, Scan Man came up with arguments of his own, starting off with the dates printed in Phrack VIII. He claimed that the dates were off and backed this up by saying Ben Graves had been fired six months previously to the conversation with Sally Ride. Scan Man then went on to ask why it had taken Sally Ride so long to come forward with his information. Scan Man made one last comment, "It's a fucking shame that there is a social structure in the phreak world!" Meaning Sally Ride merely presented his information to give himself a boost socially in the phreak world.

This is how it ended. We would like to say that TeleComputist printed the statement by Scan Man to offer both sides of the story. We make no judgements here and take no sides.

Reprinted with permission from TeleComputist Newsletter Issue 2

- -

Ok, that was Scan Man's side to the story, now that he had a few months to come up with one. Lets do a critical breakdown;

-*- "He was flown in from Charleston, West Virginia to New York every week for a four to five day duration."

Gee, wouldn't that get awfully expensive? Every week...and "made available a leased executive apartment..." He must have been quite an asset to "Telecom Management" for them to spend such large amounts on him. Kinda interesting that he lived in Charleston, West Virginia (where surprisingly enough there is a branch of TMC) and flew to New York every week.

-*- "Scan Man claimed to have no ties with TMC in Las Vegas..." Ok, I'll buy that. Notice how he didn't say that he had no ties with TMC in Charleston. Furthermore if he had no ties with TMC in Charleston why would they have his name in their company records? Why would all those employees know him or dislike him for that matter?

-*- "Scan Man then went on to say that the same day Sally Ride called Pauline Frazier was the day he received his notice." Well now, how can there be a connection between the two events at all when Scan Man works for Telecom Management and has "no ties with TMC" and claimed "not to work for TMC"? If TMC and Telecom Management are truly independent of each other then nothing Sally Ride said to Pauline Frazier could have affected him in ANY way. That is unless he did work for TMC in the first place.

-*- "...and back this up by saying that Ben Graves had been fired six months previously to the conversation with Sally Ride." Well first of all, PWN did not give a date as to when Ben Graves was fired from TMC. Second of all and more important, how does Scan Man know so much about TMC when he works for "Telecom Management" and has "...no ties with TMC..."?

The rest of his statements were highly debatable and he showed no proof as to their validity. As for why Sally Ride waited so long to come forward, well he didn't wait that long at all, he came forward to myself in late May/early June of 1986. My decision was to do nothing because there wasn't enough proof. After three months of research we had enough proof and the article was released.

With this attempt to cover up the truth, Scan Man has only given more ammunition to the idea that he isn't what he claims to be.

Special Thanks to TeleComputist Newsletter

The Cracker Cracks Up? December 21, 1986

"Computer 'Cracker' Is Missing -- Is He Dead Or Is He Alive"

By Tom Gorman of The Los Angeles Times

ESCONDIDO, Calif. -- Early one morning in late September, computer hacker Bill Landreth pushed himself away from his IBM-PC computer -- its screen glowing with an uncompleted sentence -- and walked out the front door of a friend's home here.

He has not been seen or heard from since.

The authorities want him because he is the "Cracker", convicted in 1984 of breaking into some of the most secure computer systems in the United States, including GTE Telemail's electronic mail network, where he peeped at NASA Department of Defense computer correspondence.

He was placed on three years' probation. Now his probation officer is

wondering where he is.

His literary agent wants him because he is Bill Landreth the author, who already has cashed in on the successful publication of one book on computer hacking and who is overdue with the manuscript of a second computer book.

The Institute of Internal Auditors wants him because he is Bill Landreth the public speaker who was going to tell the group in a few months how to make their computer systems safer from people like him.

Susan and Gulliver Fourmyle want him because he is the eldest of their eight children. They have not seen him since May 1985, when they moved away from Poway in northern San Diego county, first to Alaska then to Maui where they now live.

His friends want him because he is crazy Bill Landreth, IQ 163, who has pulled stunts like this before and "disappeared" into the night air -- but never for more than a couple of weeks and surely not for 3 months. They are worried.

Some people think Landreth, 21, has committed suicide. There is clear evidence that he considered it -- most notably in a rambling eight-page discourse that Landreth wrote during the summer.

The letter, typed into his computer, then printed out and left in his room for someone to discover, touched on the evolution of mankind, prospects for man's immortality and the defeat of the aging process, nuclear war, communism versus capitalism, society's greed, the purpose of life, computers becoming more creative than man and finally -- suicide.

The last page reads:

"As I am writing this as of the moment, I am obviously not dead. I do, however, plan on being dead before any other humans read this. The idea is that I will commit suicide sometime around my 22nd birthday..."

The note explained:

"I was bored in school, bored traveling around the country, bored getting raided by the FBI, bored in prison, bored writing books, bored being bored. I will probably be bored dead, but this is my risk to take."

But then the note said:

"Since writing the above, my plans have changed slightly.... But the point is, that I am going to take the money I have left in the bank (my liquid assets) and make a final attempt at making life worthy. It will be a short attempt, and I do suspect that if it works out that none of my current friends will know me then. If it doesn't work out, the news of my death will probably get around. (I won't try to hide it.)"

Landreth's birthday is December 26 and his best friend is not counting on seeing him again.

"We used to joke about what you could learn about life, especially since if you don't believe in a God, then there's not much point to life," said Tom Anderson, 16, a senior at San Pasqual High School in Escondido, about 30 miles north of San Diego. Anderson also has been convicted of computer hacking and placed on probation.

Anderson was the last person to see Landreth. It was around September 25 -- he does not remember exactly. Landreth had spent a week living in Anderson's home so the two could share Landreth's computer. Anderson's IBM-PC had been confiscated by authorities, and he wanted to complete his own book.

Anderson said he and Landreth were also working on a proposal for a movie about their exploits.

"He started to write the proposal for it on the computer, and I went to take a shower," Anderson said. "When I came out, he was gone. The proposal was in mid-sentence. And I haven't seen him since."

Apparently Landreth took only his house key, a passport, and the clothes on his back.

Anderson said he initially was not concerned about Landreth's absence. After all this was the same Landreth who, during the summer, took off for Mexico without telling anyone -- including friends he had seen just the night before -- of his departure.

But concern grew by October 1, when Landreth failed to keep a speaking engagement with a group of auditors in Ohio, for which he would have received $1,000 plus expenses. Landreth may have kept a messy room and poor financial records, but he was reliable enough to keep a speaking engagement, said his friends and literary agent, Bill Gladstone, noting that Landreth's second manuscript was due in August and had not yet been delivered.

But, the manuscript never came and Landreth has not reappeared.

Steve Burnap, another close friend, said that during the summer Landreth had grown lackadaisical toward life. "He just didn't seem to care much about anything anymore."

Typed for PWN by Druidic Death
From The Dallas Times Herald

Beware The Hacker Tracker December, 1986

By Lamont Wood of Texas Computer Market Magazines

If you want to live like a spy in your own country, you don't have to join the CIA or the M15 or the KGB. You can track hackers, like John Maxfield of Detroit.

Maxfield is a computer security consultant running a business called BoardScan, which tracks hackers for business clients. He gets occasional death threats and taunting calls from his prey, among whom he is known as the "hacker tracker," and answers the phone warily.

And although he has received no personal harassment, William Tener, head of data security for the information services division of TRW, Inc., has found it necessary to call in experts in artificial intelligence from the aerospace industry in an effort to protect his company's computer files. TRW is a juicy target for hackers because the firm stores personal credit information on about 130 million Americans and 11 million businesses -- data many people would love to get hold of.

Maxfield estimates that the hacker problem has increased by a factor of 10 in the last four years, and now seems to be doubling every year. "Nearly every system can be penetrated by a 14-year old with $200 worth of equipment," he complains. "I have found kids as young as nine years old involved in hacking. If such young children can do it, think of what an adult can do."

Tener estimates that there are as many as 5,000 private computer bulletin boards in the country, and that as many as 2,000 are hacker boards. The rest are as for uses as varied as club news, customer relations, or just as a hobby. Of the 2,000 about two dozen are used by "elite" hackers, and some have security features as good as anything used by the pentagon, says Maxfield.

The number of hackers themselves defies estimation, if only because the users of the boards overlap. They also pass along information from board to board. Maxfield says he has seen access codes posted on an east coast bulletin board that appeared on a west coast board less than an hour later, having passed through about ten boards in the meantime. And within hours of the posting of a new number anywhere, hundreds of hackers will try it.

"Nowadays, every twerp with a Commodore 64 and a modem can do it, all for the ego trip of being the nexus for forbidden knowledge," sighs a man in New York City, known either as "Richard Cheshire" or "Chesire Catalyst" -- neither is his real name. Cheshire was one of the earliest computer hackers, from the days when the Telex network was the main target, and was the editor of TAP, a

newsletter for hackers and phone "phreaks". Oddly enough, TAP itself was an early victim of the hacker upsurge. "The hacker kids had their bulletin boards and didn't need TAP -- we were technologically obsolete," he recalls.

So who are these hackers and what are they doing? Tener says most of the ones he has encountered have been 14 to 18 year old boys, with good computer systems, often bright, middle class, and good students. They often have a reputation for being loners, if only because they spend hours by themselves at a terminal, but he's found out-going hacker athletes.

But Maxfield is disturbed by the sight of more adults and criminals getting involved. Most of what the hackers do involves "theft of services" -- free access to Compuserve, The Source, or other on-line services or corporate systems. But, increasingly, the hackers are getting more and more into credit card fraud.

Maxfield and Cheshire describe the same process -- the hackers go through trash bins outside businesses whose computer they want to break into looking for manuals or anything that might have access codes on it. They may find it, but they also often find carbon copies of credit card sales slips, from which they can read credit card numbers. They use these numbers to order merchandise -- usually computer hardware -- over the phone and have it delivered to an empty house in their neighborhood, or to a house where nobody is home during the day. Then all they have to do is be there when the delivery truck arrives.

"We've only been seeing this in the last year," Maxfield complains. "But now we find adults running gangs of kids who steal card numbers for them. The adults resell the merchandise and give the kids a percentage of the money."

It's best to steal the card number of someone rich and famous, but since that's usually not possible it's a good idea to be able to check the victim's credit, because the merchant will check before approving a large credit card sale. And that's what makes TRW such a big target -- TRW has the credit files. And the files often contain the number of any other credit cards the victim owns, Maxfield notes.

The parents of the hackers, meanwhile, usually have no idea what their boy is up to -- he's in his room playing, so what could be wrong? Tener recalls a case where the parents complained to the boy about the high phone bill one month. And the next month the bill was back to normal. And so the parents were happy. But the boy had been billing the calls to a stolen telephone company credit card.

"When it happens the boy is caught and taken to jail, you usually see that the parents are disgruntled at the authorities -- they still think that Johnny was just playing in his bedroom. Until, of course, they see the cost of Johnny's play time, which can run $50,000 to $100,000. But outside the cost, I have never yet seen a parent who was really concerned that somebody's privacy has been invaded -- they just think Johnny's really smart," Tener says.

TRW will usually move against hackers when they see a TRW file or access information on a bulletin board. Tener says they usually demand payment for their investigation costs, which average about $15,000.

Tales of the damage hackers have caused often get exaggerated. Tener tells of highly publicized cases of hackers who, when caught, bragged about breaking into TRW, when no break-ins had occurred. But Maxfield tells of two 14-year old hackers who were both breaking into and using the same corporate system. They had an argument and set out to erase each other's files, and in the process erased other files that cost about a million dollars to replace. Being juveniles, they got off free.

After being caught, Tener says most hackers find some other hobby. Some, after turning 18, are hired by the firms they previously raided. Tener says it rare to see repeat offenders, but Maxfield tells of one 14-year-old repeat offender who was first caught at age 13.

Maxfield and Tener both make efforts to follow the bulletin boards, and Maxfield even has a network of double agents and spies within the hacker

community. Tener uses artificial intelligence software to examine the day's traffic to look for suspicious patterns. TRW gets about 40,000 inquiries an hour and has about 25,000 subscribers. But that does not address the underlying problem.

"The real problem is that these systems are not well protected, and some can't be protected at all," Maxfield says.

Cheshire agrees. "A lot of companies have no idea what these kids can do to them," he says. "If they would make access even a little difficult the kids will go on to some other system." As for what else can be done, he notes that at MIT the first thing computer students are taught is how to crash the system. Consequently, nobody bothers to do it.

But the thing that annoys old-timer Cheshire (and Maxfield as well) is that the whole hacker-intruder-vandal-thief phenomenon goes against the ideology of the original hackers, who wanted to explore systems, not vandalize them. Cheshire defines the original "hacker ethic" as the belief that information is a value-free resource that should be shared. In practice, it means users should add items to files, not destroy them, or add features to programs, rather than pirate them.

"These kids want to make a name for themselves, and they think that they need to do something dirty to do that. But they do it just as well by doing something clever, such as leaving a software bug report on a system," he notes.

Meanwhile, Maxfield says we are probably stuck with the problem at least until the phone systems converts to digital technology, which should strip hackers of anonymity by making their calls easy to trace.

Until someone figures out how to hack digital phone networks, of course. -TCM

Typed for PWN by Druidic Death

==Phrack Inc.==

Volume Two, Issue Eleven, Phile #12 of 12

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                                     PWN
PWN                      *>=-{ Phrack World News }-=<*                  PWN
PWN                                                                     PWN
PWN                                Issue XI                             PWN
PWN                                                                     PWN
PWN                      Written, Compiled, and Edited                  PWN
PWN                           by Knight Lightning                       PWN
PWN                                                                     PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Computer Bulletin Boards January 8, 1986

By The KTVI Channel 2 News Staff in St. Louis

Please keep in mind that Karen and Russ are anchor persons at KTVI.
All comments in []s are by me.-KL

- -

Karen: If Santa Claus brought you a computer for Christmas, beware of seeing a few things you may not have bargained for. Computer bulletin boards have spread by the thousands over the past few years and now some people are concerned that the electronic messages may have gotten a bit out of hand.

Russ: In its simplest definition, a computer bulletin board is a program or message that can be accessed by other computers via telephone lines. Anyone who has a home computer and a modem can receive and transmit to computer bulletin boards. There are thousands of them nationwide, but some are causing quite a stink [What a profound statement Russ].

[Flash to a picture of a geeky looking teenager]

Meet Jason Rebbe, he is a 16 year old computer whiz who a few months ago accidentally tapped into a bulletin board called Dr. Doom's Castle. [Sorry to break in here Russ, but why is this guy a computer whiz? Just because he has a computer? Hey Russ, look a little closer, isn't Jason sitting in front of a Commodore-64? I thought so. Oh yeah one other thing, this BBS Dr. Doom's Castle has no known relation to Dr. Doom (512) or Danger Zone Private.] Dr. Doom gives instructions on how to build bombs and guns [Lions and Tigers and Bears, oh my!]. Jason found the recipe for smoke bombs and tried to make one in his kitchen, it didn't work. [Ba ha ha].

Jason: I heard an explosion in the basement first and that's when I knew something was wrong. I thought it would be really neat to just set it off someday when there was a lot of people around, just as a joke or a prank. [Yeah, that would be K-Rad d00d!]. I didn't expect it to blow up my house.

Russ: Jason wasn't hurt, but it cost about 2 grand [that's $2,000 to you and me] to repair the kitchen. Jason's dad didn't take it well.

Bob Holloway: Mad wasn't the word for it. I, I was, I was past mad.

Russ: Mr. Holloway called Southwestern Bell and AT&T to see what could be done about bulletin boards like Dr. Doom's Castle. The answer was nothing. The Bureau of Alcohol, Tobacco, and Firearms said the same thing.

Daniel Hoggart (Bureau of Alcohol, Tobacco, and Firearms): There is no violation in publishing the information. The violation only occurs when someone actually follows through on the instructions and actually constructs a bomb.

Russ: Another bulletin board that is becoming more and more prevalent these days is the Aryian Nation. This one [bulletin board] in Chicago says,

"If you are an anti-Communist you have made the right connection...on the other hand, if you are consumed with such myths as Judeo-Christianity, you most definitely dialed the wrong number."

Stan Anderman (Anti-Defamation League): Some of this really extreme hatred is an attempt to create an environment where violence becomes acceptable.

Russ: Like most computer bulletin boards the Aryian Nation message is legal and falls under free speech laws. However, a bill is scheduled to go to congress this session outlawing the kinds of bulletin boards we saw here tonight.

But, for the moment, hackers should not be too surprised if something unusual pops up on their computer terminal. [Ahem, Russ, you did it again. All computer users are *NOT* hackers.]

Typed For PWN's Usage by Knight Lightning

MIT Unix: Victim or Aggressor? January 23 - February 2, 1987

Is the MIT system an innocent victim of hacker oppression or simply another trap to capture unsuspecting hackers in the act?

It all started like this...

[Some posts have been slightly edited to be relevant to the topic]

MIT
Name: Druidic Death
Date: 12:49 am Mon Jan 20, 1986

Lately I've been messing around on MIT's VAX in there Physics Department.

Recently some one else got on there and did some damage to files. However MIT told me that they'll still trust us to call them. The number is:

617-253-XXXX

We have to agree to the following or we will be kicked off, they will create a "hacker" account for us.

<1> Use only GUEST, RODNEY, and GAMES. No other accounts until the hacker one is made. There are no passwords on these accounts.

<2> Make sure we log off properly. Control-D. This is a UNIX system.

<3> Not to call between 9 AM and 5 PM Eastern Standard Time. This is to avoid tying up the system.

<4> Leave mail to GEORGE only with UNIX questions (or C). And leave our handles so he'll know who we are.

Unix
Name: Celtic Phrost
Date: 4:16 pm Mon Jan 20, 1986

Thanks Death for the MIT computer, I've been working on getting into them for weeks. Here's another you can play around with:

617/258-XXXX
login:GUEST

Or use a WHO command at the logon to see other accounts, it has been a long time since I played with that system, so I am unsure if the GUEST account still works, but if you use the WHO command you should see the GUEST account needed for applying for your own account.

-Phrost

Unix
Name: Celtic Phrost
Date: 5:35 pm Mon Jan 20, 1986

Ok, sorry, but I just remembered the application account, its: OPEN
Gawd, I am glad I got that off my chest!

-(A relieved)Celtic Phrost.

Also on that MIT computer Death listed, some other default accounts are:

LONG MIKE GREG NEIL DAN

Get the rest yourself, and please people, LEAVE THEM UNPASSWORDED!

MIT
Name: Druidic Death #12
Date: 1:16 am Fri Jan 23, 1987

MIT is pretty cool. If you haven't called yet, try it out. Just PLEASE make sure you follow the little rules they asked us about! If someone doesn't do something right the sysop leaves the gripe mail to me. Check out my directory under the guest account just type "cd Dru". Read the first file.

MIT
Name: Ctrl C
Date: 12:56 pm Sat Jan 24, 1987

MIT Un-Passworded Unix Accounts: 617-253-XXXX

ALEX BILL GAMES DAVE GUEST DAN GREG MIKE LONG NEIL TOM TED
BRIAN RODNEY VRET GENTILE ROCKY SPIKE KEVIN KRIS TIM

And PLEASE don't change the Passwords....

-=>Ctrl C<=-

MIT Again
Name: Druidic Death
Date: 1:00 pm Wed Jan 28, 1987

Ok people, MIT is pissed, someone hasn't been keeping the bargain and they aren't too thrilled about it. There were only three things they asked us to do, and they were reasonable too. All they wanted was for us to not compromise the security much more than we had already, logoff properly, not leave any processes going, and call only during non-business hours, and we would be able to use the GUEST accounts as much as we like.

Someone got real nice and added themselves to the "daemon" group which is superusers only, the name was "celtic". Gee, I wonder who that could have been? I'm not pissed at anyone, but I'd like to keep on using MIT's computers, and they'd love for us to be on, but they're getting paranoid. Whoever is calling besides me, be cool ok? They even gave me a voice phone to chat with their sysops with. How often do you see this happen?

a little perturbed but not pissed...

DRU'

Tsk, Celtic.
Name: Evil Jay
Date: 9:39 am Thu Jan 29, 1987

Well, personally I don't know why anyone would want to be a superuser on the system in question. Once you've been on once, there is really nothing that

interesting to look at...but anyway.

-EJ

In trouble again...
Name: Celtic Phrost
Date: 2:35 pm Fri Jan 30, 1987

...I was framed!! I did not add myself to any "daemon" group on any MIT UNIX. I did call once, and I must admit I did hang up without logging off, but this was due to a faulty program that would NOT allow me to break out of it, no matter what I tried. I am sure that I didn't cause any damage by that.

-Phrost

Major Problems
Name: Druidic Death
Date: 12:20 pm Sat Jan 31, 1987

OK, major stuff going down. Some unidentified individual logged into the Physics Dept's PDP11/34 at 617-253-XXXX and was drastically violating the "agreement" we had reached. I was the one that made the "deal" with them. And they even gave me a voice line to talk to them with.

Well, one day I called the other Physics computer, the office AT and discovered that someone created an account in the superuser DAEMON group called "celtic". Well, I was contacted by Brian through a chat and he told me to call him. Then he proceeded to nicely inform me that "due to unauthorized abuse of the system, the deal is off".

He was cool about it and said he wished he didn't have to do that. Then I called George, the guy that made the deal and he said that someone who said he was "Celtic Phrost" went on to the system and deleted nearly a year's worth of artificial intelligence data from the nuclear fission research base.

Needless to say I was shocked. I said that he can't believe that it was one of us, that as far as I knew everyone was keeping the deal. Then he (quite pissed off) said that he wanted all of our names so he can report us to the FBI. He called us fags, and all sorts of stuff, he was VERY!! [underline twice] PISSED! I don't blame him. Actually I'm not blaming Celtic Phrost, it very easily could have been a frame up.

But another thing is George thinks that Celtic Phrost and Druidic Death are one and the same, in other words, he thinks that *I* stabbed him in the back. Basically he just doesn't understand the way the hacker community operates.

Well, the deal is off, they plan to prosecute whoever they can catch. Since George is my best friend's brother I have not only lost a friend, but I'm likely to see some legal problems soon. Also, I can forget about doing my graduate work at MIT. Whoever did this damage to them, I hope you're happy. You really messed things up real nice for a lot of people.

Celtic, I don't have any reason to believe you messed with them. I also have no reason to think you didn't. I'm not making an accusation against you, but WHOEVER did this, deserves to be shot as far as I'm concerned. Until this data was lost, they were on the verge of harnessing a laser-lithium produced form of nuclear fission that would have been more efficient than using the standard hydrogen. Well, back to the drawing board now.

I realize that it's hard to believe that they would have data like this on this system. But they were quite stupid in many other areas too. Leaving the superuser account with no password?? Think about it.

It's also possible that they were exaggerating. But regardless, damage seems to have been done.

MIT
Name: Phreakenstein
Date: 1:31 am Sun Feb 01, 1987

Heck! I dunno, but whoever it was, I think, should let himself (the s00per K-rad elyte d00d he is) be known.

I wasn't on MIT, but it was pretty dumb of MIT to even let Hackers on. I wouldn't really worry though, they did let you on, and all you have to prove is that you had no reason to do it.

----Phreak

I wonder...
Name: Ax Murderer #15
Date: 6:43 pm Sun Feb 01, 1987

I highly doubt that is was someone on this system. Since this is an elite board, I think all the users are pretty decent and know right and wrong things to do. Could be that one of the users on this system called another system and gave it out!?? Nahh...shooting the asshole is not enough, let's think of something better.

Ax Murderer

It was stupid
Name: Druidic Death #12
Date: 9:21 pm Sun Feb 01, 1987

It seems to me, or, what I gathered, they felt that there were going to be hackers on the system to begin with and that this way they could keep themselves basically safe.

I doubt that it was Celtic Phrost, I don't think he'd be an asshole like that. But I can't say. When I posted, I was pretty pissed about the whole deal. I've calmed down now. Psychic Warlord said something to me voice the other day that made me stop and think. What if this was a set up right from the start? I mean, MIT won't give me specifics on just what supposedly happened, Celtic Phrost denies everything, and the biggest part of it is what George said to me.

"We can forgive you for what you did to us if you'll promise to go straight and never do this again and just tell us who all of your friends are that are on the system".

I didn't pay much attention to that remark at first, now I'm beginning to wonder...

I, of course, didn't narc on anyone. (Who do I know??? hehe)

DRU'

Well
Name: Solid State
Date: 11:40 pm Sun Feb 01, 1987

Well if they were serious about the FBI, I wouldn't take this too lightly. Lately at Stanford there has been a lot of investigators that I've pinpointed running around. This is mainly due to the number of break-ins this summer.

Anyways, if a large college like MIT says they may call in the FBI, be wary, but don't over-react.

SOLID STATE

Comments...
Name: Delta-Master
Date: 7:15 am Mon Feb 02, 1987

It wouldn't surprise me if it was some kind of setup, it's been done before.

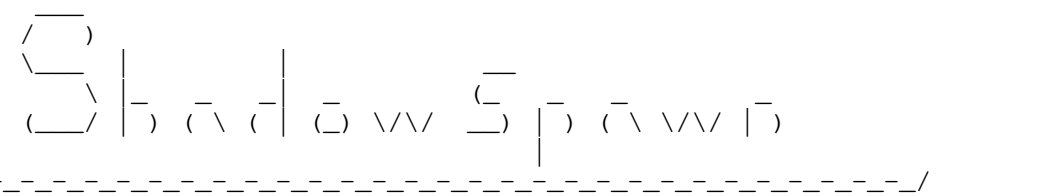
Delta-Master

Oh well...
Name: Evil Jay
Date: 8:56 am Mon Feb 02, 1987

I think your all wrong. The MIT lines have been around for a long time and are widely known among the rodents. Anyone with a g-file could hack out a password on the system so it looks to me like someone just messed around and just happened to use Phrost as a flunkie. Oh well...

-EJ

All posts taken from:



"We're not ELITE... we're just cool as hell."

- -

Information Provided indirectly/directly by

Ax Murderer/Celtic Phrost/Ctrl C/Delta-Master/Druidic Death
Evil Jay/Phreakenstein/Solid State

Phortune 500: Phreakdom's Newest Organization February 16, 1987

For those of you who are in the least bit interested, Phortune 500 is a group of telecommunication hobbyists who's goal is to spread information as well as further their own knowledge in the world of telecommunications. This new group was formed by:

Brew Associates/Handsomest One/Lord Lawless/The Renegade Chemist
Quinton J. Miranda/Striker/The Mad Hacker/The Spiker

These eight members are also known as Board Of Directors (BOD). They don't claim to be *Elite* in the sense that they are they world's greatest hackers, but they ARE somewhat picky about their members. They prefer someone who knows a bit about everything and has talents exclusive to him/herself.

One of the projects that Phortune 500 has completed is an individual password AE type system. It's called TransPhor. It was written and created by Brew Associates. It has been Beta tested on The Undergraduate Lounge (Sysoped by Quinton J. Miranda). It is due to be released to the public throughout the next few months.

Phortune 500 has been in operation for about 4 months, and has released two newsletters of their own. The Phortune 500 Newsletter is quite like the "People" of contemporary magazines. While some magazines cover the deep technical aspects of the world in which we communicate, their newsletter tries to cover the lighter side while throwing in information that they feel is "of technical nature." The third issue is due to be released by the end of this month.

- -

>=-> The Phortune 500 Membership Questionnaire <-=<

Note: The following information is of a totally confidential nature. The reason you may find this so lengthy and in depth is for our knowledge of you. We, with Phortune 500, feel as though we should know prospective members well before we allow them into our organization. Pending the answers you supply us, you will be admitted to Phortune 500 as a charter member. Please answer the following completely...

.....

Handle :
First Name :
Voice Phone Number :

```
Data Phone Number               :
City & State                    :
Age                             :
Occupation (If Applicable)      :
Place of Employment (Optional)  :
Work Phone Number   (Optional)  :
Computer Type                   :
Modem Type                      :
Interests                       :
Areas Of Expertise              :
References (No More Than Three) :
Major Accomplishments (If Any)  :
.....................................................................
Answer In 50 Words Or Less;

^*^  What Is Phortune 500 in Your Opinion?

^*^  Why Do You Want To Be Involved With Phortune 500?

^*^  How Can You Contribute to Phortune 500?
.....................................................................

Please answer each question to the best of your ability and then return to any
Phortune 500 Board of Directors Member Or a Phortune 500 BBS:

          The Private Connection (Limited Membership) 219-322-7266
          The Undergraduate AE   (Private Files Only) 602-990-1573

                        Information provided by

             Quinton J. Miranda & Phortune 500 Board Of Directors
```

PWN Quicknote

At the University of Rhode Island there is supposed to be some undercover agent for Bay Bell. Supposedly he hangs out at the library and watches for people checking out the Bell Technical Journals. Then he asks questions like, 'What do you want those for?' 'Do you know what 2600Hz is?' and other similar questions. He isn't registered at the school and of course has no classes. [Sounds bogus to me...oh well-KL]. Information by Asmodeus Rex (1/21/87)

==Phrack Inc.==

Volume Two, Issue Eleven, Phile #2 of 12

==Phrack Pro-Phile VIII==

Written and Created by Taran King

2/17/87

Welcome to Phrack Pro-Phile VIII. Phrack Pro-Phile is created to bring info to you, the users, about old or highly important/controversial people. This month, I bring to you one of the older and high profile phreaks of the past...

Wizard of Arpanet

Wizard of Arpanet is one of the older of the phreak/hack generation. His main accomplishments include running Inner Circle and Secret Service BBS.

Handle:	Wizard of Arpanet
Call him:	Eric
Past handles:	The Hacker and The Priest
Handle Origin:	A real programmer on Arpanet was called The Wizard and Eric took his handle from him.
Date of Birth:	02/26/69
Age in 9 days of this writing:	18 years old
Height:	6'1"
Weight:	150 lbs
Eye color:	Blue
Hair color:	Dishwaterish blond
Computers:	Atari 400, Commodore 64
Sysop/Co-sysop of:	Secret Service

Wizard of Arpanet started as your average BBS caller. He eventually called Central Processing Unit (a local board to him), and there were these funny numbers on the board. He called and tried to connect with his modem, but they turned out to be Sprint dial-ups. The CPU Sysop informed him of what to do and he started calling national BBSs. Boards that helped him to advance include the Twilight Zone (the sysop was the guy that wrote T-Net), OSUNY, Dragon's Lair, and Delta BBS. Wizard organized various groups which included (from earliest to most recent): PHA (Phreakers and Hackers of America) - (included Deep Throat, Phreak King, and Psycho Killer), The Inner Circle (1st one) (included Shockwave Rider, and Satan Knight aka Redrum), and The 2nd Inner Circle (included The Cracker, Mr. America, Napoleon Bonapart, Stainless Steal Rat, Big Brother, Mr. Xerox, Bootleg, Maxwell Wilke, Mandrake The Magician, and Zaphod Beeblebrox).

Eric got the number to Arpanet from Dark Dante, and got on the MIT Research System from looking through TAC News. One night he got like 50-60 accounts on the Unix and changed all of the passwords to WIZARD.

Stainless Steal Rat, the Sysop of Delta BBS, and The Myth were all up from NJ one weekend, and they were staying the weekend at John Maxfield's house. They went to John's office. Wizard asked Maxfield if he could use his computer to print out some things he had with him and he printed out some stuff from the Stanford Artificial Intelligence address list for Arpanet. John was amazed. "Wow," he said, "I have prime evidence on you." (TK: This may not for sure be an exact quote). He then proceeded to bust our friend, Eric, the next week. He also had a lot of stuff from AUTOVON from some fellow in Washington and started playing with the FTS lines (Federal Telephone System) which he found from, none other than, John Maxfield. They had found the default passwords for TeleMail too, and got the administrator accounts and set up their own BBS on Nassau and Coca-Cola systems plus anywhere else possible. And all of a sudden, it all came down when Mandrake decided to crash parts of TeleMail. Enter, Federal Bureau of Investigations. They had been monitoring Eric for 6 months looking for some evidence to get him on. And thus, they got it. Nothing really happened, but he had to get a lawyer

and he got some publicity in the paper. After 90 days, everything they had taken, with the exception of a few documents, was sent back. During those 90 days, Eric worked as a computer security consultant at a bank making $200 an hour (2 hours...).

The only "phreaks" he's met are Stainless Steal Rat and Cable Pair.

Eric has been mentioned on local TV/News, in newspapers, USA Today, NY Times, Washington Post, Books, and Britannica Encyclopedia (look under Hacker).

Interests: Music (preferably jazz, reggae, new wave), Eastern philosophy (Zen Buddhism), reading Jack Kerouac books (a great beatnik writer), driving aimlessly, slowly becoming a social recluse, physics, and Greek mathematicians.

Eric's Favorite Things

Women: The pursuit thereof (Karen Wilder).
Foods: Chinese.
Cars: BMW 320-I.
Artist: Salvador Dali.
Plans for next few months: Next year and a half - travelling to Montreal in April for a week of leisure, then jetting back to beautiful Detroit and continuing his studies at Eisenhower High School.

Most Memorable Experiences

Realizing all at once that everything you did 3 years ago was stupid.
Growing into a new person.
Gaining morals and new ideas and a new outlook.

Some People to Mention

Tuc (For telling him about boxing).
Tom Tone (For calling him on his first conference).
Magnetic Surfer (Talking to him for the first time after Sherwood Forest went down voice).
John Maxfield (Meeting him).
Stainless Steal Rat (Meeting him...with John Maxfield).
Dark Dante (One of the legends phreakdom).

Always follow your instinct and not your desire for you will be sorry because you will be lying to yourself.

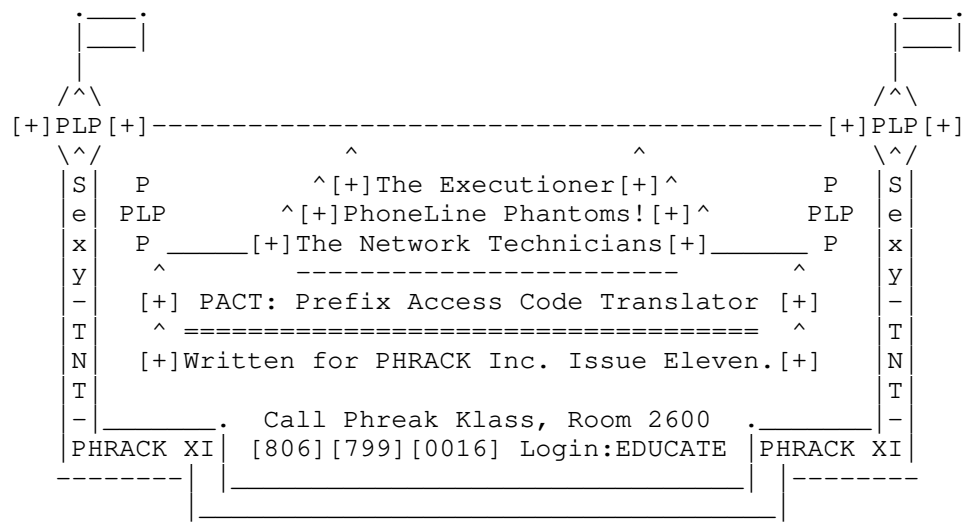
I hope you enjoyed this file. Look forward to more Phrack Pro-Philes coming in the near future. ...And now for the regularly taken poll from all interviewees.

Of the general population of phreaks you have met, would you consider most phreaks, if any, to be computer geeks? No, says Eric, he considers them a new breed of intellect. Thanks for your time, Eric.

Taran King
Sysop of Metal Shop Private

==Phrack Inc.==

Volume Two, Issue Eleven, Phile #3 of 12



The PACT (Prefix Access Code Translator) feature provides preliminary translation data for features using access codes that are prefixed by a special code. A standard numbering and dialing plan requires that individual line and small business customers' (custom) calling use prefixed access code dialing for feature access. PACT is offered on a per office basis. The PACT is NOT used for the interpretation of Centrex dialing customers.

When a call is originated by the customer, a call register is used to store the data about the call. The customer dials a prefix and a 2 digit access code (table a). The PACT then looks at the digits to determine what action should take place. Reorder or special service error messages will be heard if you enter an unassigned code. If the code is accepted, then that particular action will be performed. The PACT consists of the PACT head table and the prefixed access code translator. The PACT feature allows the dialing of a special code for a prefix. These are the '*' and '#'. If you have rotary, then '11' and '12' are used respectively. To use PACT, the prefix must be followed by a 2-digit code. This combination is then defined in terms of type and subtype (table b).

TABLE A

Access Code	Description of function
*2X - *3X (x= 0-9)	Growth to 2 or 3 digit codes (Future may call for these)
*4X - *5X - *7X	Local Area Signalling Services
*72	Call Forwarding Activation
*73	Call Forwarding Deactivation
*74	1-digit speed dialing
*75	2-digit speed dialing
#56	Circuit Switched Digital Capability

The subtranslator is always built 100 words long. A word is a binary code which, when sent as a whole, act as a command. One word is equal to a 2-digit access code. This subtranslator contains the PTW (Primary Translation Word). The PTW contains the feature type subtype and feature subtype index to determine the function of the dialed code. The feature subtype allows four subtype tables to exist for feature type 31 (LASS). Index 0 is for LASS. Index 1 is used for LASS on a pay per usage basis. Index 2 and 3 are currently not

used.

TABLE B (written in report form)
==========

Feature Type: 0 (Unassigned)

Feature Type: 1 (1-digit abbr. dialing)

Subtypes: 0 (Speed Call)
1 (Change the Speed Call List)
2 (Invalid)

Feature Type: 2 (2-digit dialing.)

Subtypes: (Same as Feature 1)

Feature Type: 3 (Circuit Switch Digital Capability)

Subtype: 1 (CSDC 56 kilo bit service)

Feature Type: 4 (Usage Sensitive 3-way)

Feature Type: 5 (Cancel Call Waiting)

Feature Type: 20 (Call Forwarding Activate)

Feature Type: 21 (Call Forwarding deactivate)

Feature Type: 22 (Project Acct. Service (Autoplex))

Feature Type: 26 (Customer changeable Inter LATA carrier)

Feature Type: 27 (Voice/Data Protection)

Feature Type: 28 (MDS-Message Desk Service)

Subtypes: 0 (MDS activation)
1 (MDS deactivation)

Feature Type: 30 (Residence Data Facility Pooling)

Feature Type: 31 (Local Area Signalling Services-LASS)
[index 0]

Subtypes: 0 (AR-Automatic Recall {Incoming Calls})
1 (AR-Outgoing calls)
2 (AR activation incoming/outgoing)
3 (AR deactivation)
4 (Customer Originated Trace Activation)
5 (Distinctive Alert Activation)
6 (ICLID activation)
7 (Selective Call Rejection Activation)
8 (Selective Call Forwarding activation)
9 (Private Call Activation)
10 (Distinctive Alert -OFF)
11 (ICLID-OFF)
12 (SCR-OFF)
13 (SCF-OFF)
14 (Private Call-OFF)
15 (Distinctive Alert ON/OFF) toggle for opposite
16 ICLID toggle on/off
17 SCR toggle on/off
18 SCF toggle on/off
19 Private Call on/off
20 Selective Call Acceptance-ON
21 SCA OFF
22 SCA toggle on/off
23 (Computer Access Restriction) on
24 CAR off

```
           25 CAR on/off
         26-31 (reserved for future LASS functions)

Index 1 Pay Per View

       subtype: 0 (Order placement)
                1 (Order Cancel)
```

The PACT function is extremely important for LASS functions. PACT is what lets you tell your switch what you want done. Without the PACT, communication between you and your CO would not exist. PACT is the base foundation for the use access codes.

```
         ============================================================
         = If you have any questions or comments, please leave mail =
         = either on Phreak Klass Room 2600 or at 214-733-5283.     =
         ============================================================
         = (c) The Executioner/PLP/TNT                              =
         ============================================================
```

==Phrack Inc.==

Volume Two, Issue Eleven, Phile #4 of 12

Hacking Voice Mail Systems

Written for Phrack XI

by:-> Black Knight from 713

Voice Mail is a relatively new concept and not much has been said about it. It is a very useful tool for the business person and the phreak. The way it works is that somebody wishing to get in touch with you calls a number, usually a 1-800, and punches in on his touch-pad your mailbox number and then he is able to leave a message for you. Business experts report that this almost totally eliminates telephone tag. When a person wishes to pick up his message all he needs to do is call the number enter a certain code and he can hear his messages, transfer them, and do other misc. mailbox utilities.

Most VMSs are similar in the way they work. There are a few different ways the VMSs store the voice. One way is that the voice is recorded digitally and compressed and when heard it is reproduced back into the voice that recorded it. Another method that is slower and uses more space, but costs less, stores the voice on magnetic tape, the same type that is used to store data on a computer, and then runs the tape at a slow speed. Using this method the voice does not need to be reproduced in any way and will sound normal as long as the tape is running at a constant speed. On some of the newer VMSs the voice is digitally recorded and is transformed from the magnetic tape at about 2400 bits per second.

There are many different types and versions of voice mail systems. Some of the best and easiest to get on will be discussed.

Centagram

These are direct dial (you don't have to enter a box number). To get on one of these, first have a number to any box on the system. All of the other boxes will be on the same prefix; just start scanning them until you find one that has a message saying that person you are calling is not available. This usually means that the box has not been assigned to anybody yet. Before the nice lady's voice tells you to leave the message, hit #. You will then be prompted for your password. The password will usually be the same as the last four digits of the box's number or a simple number like 1000, 2000, etc. Once you get on, they are very user friendly and will prompt you with a menu of options. If you can't find any empty boxes or want to do more, you can hack but the system administrators box, which will usually be 9999 on the same prefix as the other boxes, will allow you to hear anybody's messages and create and delete boxes.

Sperry Link

These systems are very nice. They will usually be found on an 800 number. These are one of the hardest to get a box on because you must hack out a user ID (different from the person's box number) and a password. When it answers, if it says, "This is a Sperry Link voice station. Please enter your user ID," you will have to start trying to find a valid user ID. On most Sperrys it will be a five digit number. If it answers and says, "This is an X answering service," you first have to hit *# to get the user number prompt. Once you get a valid user number will have to guess the password on most systems, it will be 4 digits. Once you get in, these are also very user friendly and have many different options available.

RSVP

This is probably one of the worst VMSs but it is by far the easiest to get yourself a box. When it answers you can hit * for a directory of the boxes on it (it will only hold 23). If you hit # you will be given a menu of options and when you choose an option you will then be prompted for your ID number. The ID number on an RSVP system will just about always be the same as the

mailbox number, which are always only 2 digits.

A.S.P.E.N.

The Aspen voice message systems made by Octel Telecommunications is in my opinion the BEST VMS made. To get a box on an Aspen, you need to find an empty box. To find an empty box, scan the box numbers and if one says, "You entered XXXX. Please leave a message at the tone," then this is an empty box. You next just press # and when prompted for your box number enter the number of the empty box and friendly voice of the nice lady will guide you through all of the steps of setting up your box. She first tells you what you can do with the box and then will prompt you with, "Please enter the temporary password assigned to you by your system manager." This password will usually be 4 digits long and the same as the box number like 1000, etc. Once you get on their are many things you can do. You can make a distribution list where if you want to leave a certain message to more than one person, you can enter the list number and all of the boxes on the list will get the message. You can also have the system call you and notify you that you have new messages. These systems also have what they call "Information center mailboxes" that are listen only and can also have a password on them so the person calling has to enter the password before he hears the greeting message. Aspen VMSs have a system managers mailbox that will just about give you total control of the whole system and let you listen to people's mail, create and delete boxes, and many other things.

Thank you for reading this file and if you would like to get in touch with me VIA VOICE MAIL call 1-800-222-0311 and hit *2155.

```
                    //--Black Knight from 713--\\
                    |     for PHRACK XI (1987)  |
                    \\--++--++--++--++--++--++--//
```

==Phrack Inc.==

Volume Two, Issue Eleven, Phile #5 of 12

{Simple Data Encryption}
<or digital electronics 101>

By:{The Leftist}

Prologue:

Well, it’s been awhile since I’ve done one of my activities files. This time I’ve switched from chemistry to electronics. Hopefully, I will be writing more files similar to this one. Also, I have devised a more sophisticated encryption device, which I may release in the future

Do you run a BBS, living in fear that the "feds" are gonna log on, and fool you into giving them a password? Do you wish that you could limit exactly WHO logs onto your board? Well, this file is just for you..

Parts:

1:9 volt battery

1: 74hc/hct04 cmos hex inverter <about .50 cents>

Some basic knowledge of electronics might help, and some wire would be helpful too. If you want to be fancy you can even splurge and get a 9 volt connector.

Note: Although it is not required that you put this on an etched PC board, you can do this quite easily, and it makes for a much cleaner job.

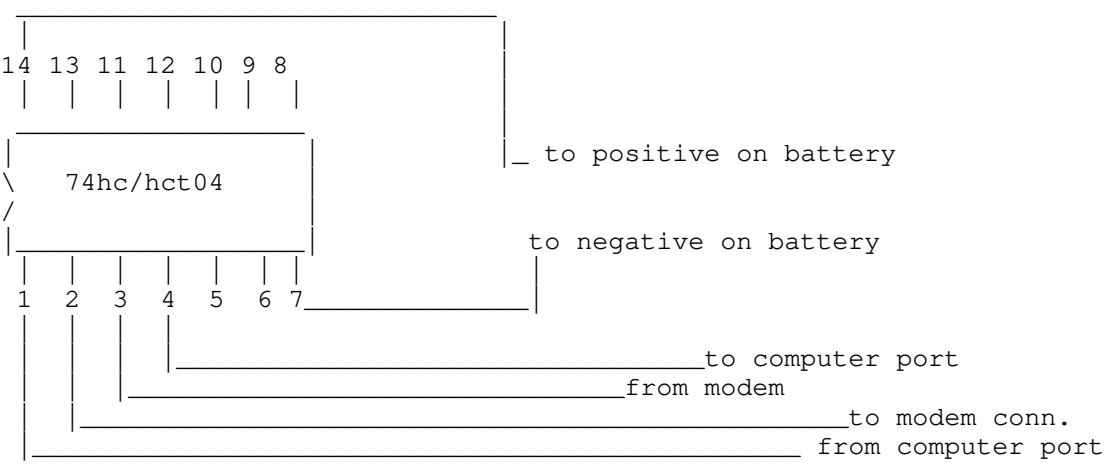
Ok, the basic idea behind this scheme is this:

Data coming to and going from your modem is translated as 1’s and 0’s. This represents highs and lows, which translate out to code which your computer recognizes as valid data. Now, if you could switch all those 1’s to 0’s, and 0’s to 1’s, then you would have a simple way of encrypting your data. That’s exactly what the hex inverter does. If it sees a 0, it makes it a 1. If it sees a 1, it makes it a 0. So, what you want to do is have an inverter on your send line, and an inverter on your receive line. The computer you are connected to must also have inverters on its send and receive, or all you will see will be garbage! I tried to be as non-technical as possible in this for all you non-technical types out there.

Connections:

Hold the chip, and look at it. There should be a little notch in one end. Hold it as illustrated in the schematic:

(80 columns)



<all other pins are not connected>

Ok, hook the + 9volts up to pin 14, and the negative up to pin 7.
There are 6 inverters on this chip. For this, we will be using only 2 of them.

Find the wire coming from your computer to the send data line on your modem. Sever this wire, and hook one side of it to pin 1. Hook the other end of it to pin 2. Next, find the receive data line, and sever it. Hook one end of it to pin 3, the other end to pin 4. That's about it.. if you want to use the other inverters on the chip, here's the complete pinouts.

Pin#	Name and function
1,3,5,9,11,13	Data inputs
2,4,6,8,10,12	Data outputs
7	Ground
14	VCC

Remember, that your BBS modem must have one of these devices on it, as well as the user calling. I have tested this on Smartmodems, and it does work. If you have an internal modem, this may be a little difficult for you.

==Phrack Inc.==

Volume Two, Issue Eleven, Phile #6 of 12

Taran King Presents...

AIS - Automatic Intercept System

The DAIS II System by Computer Consoles Incorporated

INTRODUCTION...

Computer Consoles Incorporated (CCI) manufactures various hardware appliances to be used in conjunction with phone companies switches as well as other aspects of the companies' uses, plus computer systems such as their own Unix-supporting systems.

DAIS II is the Distributed Automatic Intercept System, which is the system used to announce if the subscriber has dialed a non-working number. This is what you hear, in action, when you dial a wrong number and get the 3 tones plus the announcement or the ONI (Operator Number Identification) intercept operator ("What number did you dial?").

The information from this file comes mostly from an instructional manual sent to me by CCI, who can be reached at 800-833-7477 or 716-482-5000 directly, or may be written to at 97 Humbolt Street, Rochester, NY, 14609.

INTERCEPTION

Most definitely any person who has used a telephone in his life has, by some means or another, come across the dreaded 3 tones, leading up to the ever-so-cumbersome announcement telling of the disconnected or non-working number. This file will go into how the whole system works.

After dialing the non-working number, the telco's Class 5 End Office routes the call to DAIS II.

ANI Calls

Provided that the End Office has Automatic Number Identification (ANI) equipment, the equipment then identifies the digits of the called number and sends them to the intercept system.

The system receives the called number from the end office, retrieves information for that number from the intercept database, formulates the message, and delivers it to the customer in an automated announcement. These announcements can either be standardized or tailored to the independent telephone companies' needs. If further assistance is required, the caller can then stay on the line and wait for an operator to come onto the line.

ONI Calls

When the End Office is primitive, and they don't have the ANI equipment to do the above ritual, operators are directly involved. These operators are also called into action when there is an ANI or DAIS II failure.

When the ONI (Operator Number Identification) call comes in, DAIS II routes the call to the operator. The operator asks for the number that the customer called and then keys it into her KDT (Keyboard Display Terminal). After she hits the command key, the number's information is searched for in the intercept database, the message is formulated, and the automated response is announced. Once again, if the caller needs further assistance, an operator will return to the line to help the subscriber.

Operators will return to the line for any number of reasons. They include the following:

Unsuccessful Searches - After DAIS II receives the called number from ANI equipment or from an operator, it searches the database to find the intercept message associated with the telephone number. The database contains all 10,000 line numbers for each exchange in the calling area. If the system cannot complete the search, the number was either keyed in incorrectly or there is a problem in the system. The call is then routed to an

operator and displays the intercepted number (including NPA) on the KDT screen along with a message indicating why the search could not be completed. If the number was keyed in wrong, the operator will correct the number, or else she will ask the subscriber to re-dial the number.

Aborted Announcements - If a search is given successful but for one reason or another the automated announcement cannot be given, the call is routed to an operator. The KDT display shows the intercepted number, the appropriate information for a verbal response, and the message, "VERBAL REPORT." In this case, the operator quotes the message to the caller rather than activating the automated response.

Reconnects - If a customer remains on the line for more information after receiving the automated announcement, the system routes the call to an operator. The operator's KDT display shows the called number plus other pertinent information given to the caller in the previous announcement. From here, the operator can respond verbally to the customer's needs, or activate the automated system again. The DAIS II system allows up to 4 reconnects per call, but the possible number of reconnects available ranges from 0-3. With 1 reconnect, the operator must report verbally.

Split Referrals - If a number has been changed but replaced with two numbers, this is called a "split referral." When the database finds 2 or more numbers, the DAIS II system routes the customer to an operator, displaying the old number and new listings on the KDT screen. The operator then asks which number they are looking for and keys in the command key to activate the announcement, or else they do the announcement verbally.

Operator Searches
~~~~~~~~~~~~~~~~~

Situations may arise where the subscriber needs more information than was given by the automated announcement, or believes the information to be invalid. DAIS II provides for operators to have access to both the intercept and the DA databases at all times as long as the system administrator, who judges the extent to which operators can use the cross-search capability, allows it.

Components Of The System
~~~~~~~~~~~~~~~~~~~~~~~~

The telco's Class 5 End Offices contain switching equipment that routes calls to DAIS II. If the office has ANI equipment, the switch routes the called digits to the intercept system in the form of multi-frequency tones. The end offices route calls to DAIS II on dedicated (direct) trunks. These direct trunks can carry ANI traffic or ONI traffic, but not both.

If trunk concentrators are used, the concentrator trunks to DAIS II may carry ANI calls, ONI calls, or both, depending on the types of trunks coming into the concentrators from the end offices. The call is identified as ANI or ONI through MF tones transmitted by the concentrators.

If an operator must be involved (due to ONI or further assistance), DAIS II routes the call to the telco's ACD (Automatic Call Distributor), which is a switching device that routes calls to any available operator.

The intercept data base resides on disk in the ARS (Audio Response System). ARS processors known as Audio Response Controllers (ARCs) search the intercept database. If a call requires an operator's services, the Marker Decoder Unit (MDU) provides ACD routing information to the ARC.

The DAIS II Automatic Intercept Communications Controllers (AICCs) route messages between the ARCs and the DAIS II subsystems. An intercept subsystem that is housed at the same location as the database is called a Colocated Automated Intercept System (CAIS). A subsystem located at a

distance from the database is known as a Local Automated Intercept System (LAIS). Each subsystem can provide automated announcements without using expensive trunking to route ANI calls to a centralized intercept office. Only calls that require operator assistance are routed on trunks to the ARS site. Because those trunks are only held white the operator identifies the number and are released before the announcement begins, trunk requirements are reduced. The automated announcement is always given by the intercept subsystem.

Each CAIS or LAIS site contains a Trunk Time Switch (TTS) and DAIS II Audio Response Units (DARUs). Intercept trunks from the concentrators and the Class 5 End Offices terminate at the TTS. When an ONI call comes in on one of these trunks, the TTS routes it to the ACD. When an ANI call comes in, the TTS routes the called number to the ARC. After the ARC retrieves the appropriate message from the database, it sends that information back to the TTS, which connects a DARU port to the trunk on which the call came in. Then, the DARU produces an automated announcement of the message and delivers it to the caller. ARS hardware generates only DA announcements whereas DAIS II hardware generates only intercept announcements.

Automatic Intercept Communications Controller (AICC)
~~~~~~

The AICC routes messages between the ARC and the TTS. Two units are required to enhance system reliability. Each pair of AICCs can communicate with up to 4 CAIS or LAIS subsystems.

The AICCs are similar to the Audio Communications Controllers (ACCs) in the ARS system, but AICCs use a Bisynchronous Communications Module (BSCM) instead of a LACIM.

An AICC can be equipped with up to 8 BSCMs, each of which handles one synchronous communication line to the TTS. The BSCM models selected depend on the location of the AICC with respect to the CAIS/LAIS sites. Standard SLIMs (Subscriber Line Interface Modules) are required for communication with the ARC.

Trunk Time Switch (TTS)
~~~~~~~~~~~~~~~~~~~~~~~

The TTS has two types of components: the Peripheral Modules (PMs) and the Common Controls (CCs).

The PM contains the printed circuit boards that provide the link between the end office's ANI trunks and the ARC and between the ONI trunks and the ACD. The activity of the PM is under direction of the CC

A PM rack contains five types of circuit boards: Multi-frequency Receivers (MFRs), Analog Line Front Ends (ALFEs), T1 Front Ends (T1FEs), Peripheral Module Access Controllers (PMACs), and Multi-purpose Peripheral Devices (MPPDs).

The MFRs translate the intercepted number from multi-frequency tones to ASCII digits for ANI calls; for ONI calls that come through a trunk concentrator, the MFRs translate the tones sent by the concentrator to indicate an ONI call. Based on the tones, the MFR determines the type of call: regular, trouble, etc.

ALFEs convert incoming analog data to digital form so that it can be switched on the digital network. They also convert outgoing digital data back to analog. Incoming ALFEs provide the link between the TTS and the analog trunks from the Class 5 End Offices. Outgoing ALFEs provide the link between the TTS and the analog trunks to the ACD.

ALFE is subdivided into two types for both incoming and outgoing: ALFE-A (contains the control logic, PCM bus termination, and ports for 8 trunks) and ALFE-B (contains ports for 16 trunks, but must be paired with an ALFE-A in order to use the control logic and PCM bus on the backplane). ALFE-As can be used without ALFE-Bs, but not vice versa.

Incoming ALFEs support E&M 2-wire, E&M 4-wire, reverse battery, and 3-way signalling trunks. Outgoing ALFEs support E&M 2-wire, reverse battery, and high-low trunking.

T1FEs provide the links between the TTS and the D3-type T1 spans from the end offices. They also link the DARU VOCAL board ports and the TTS. Each board has 24 ports in order to handle a single T1 span which carries 24 voice channels.

PMAC is based on a Motorola 68000 microprocessor that directs and coordinates data flow within the PM.

MPPD boards provide bus termination and the system clocks for the digital network. The MPPD contains a master and a secondary clock, which are synchronized with the frequency of an incoming T-1 span. The module also contains its own clock for use when T-1 synchronization is not available or lost.

The MPPD also generates the ringing tones, busy signals, and reorder tones heard by the customer and sends the zip (alert) tone to the operator.

The CC controls the interaction between the PM components and the DARU. It contains the Office Dependent Data Base (ODDB), which is a system table that describes the configuration of the TTS. The CC uses the ODDB to determine whether an incoming call is an ANI or ONI trunk.

The CC sets up paths through the digital network in order to coordinate the resources of the CAIS/LAIS. It receives messages from the PMAC, stores information necessary for returning a response to the appropriate trunk, and controls message routing to and from the ARC or the operator. It also synchronizes the TTS and the Directory Assistance System (DAS) for operator-caller communications.

The CC is a Power-series standalone processor that contains a central processing unit (CPU-2), based on the Motorola 68000 microprocessor. The processor also contains distributed intelligence for controlling the memory subsystem, the IO (input/output) subsystem, and the disk/tape subsystem. Each CC includes a Winchester disk drive, a quarter-inch tape drive, and additional miscellaneous hardware.

DAIS II Audio Response Unit (DARU)
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

The DARU contains the VOCAL boards that produce automated announcements, which are compiled from a vocabulary stored in RAM. A CAIS/LAIS contains 1 to 3 DARUs, each with 48 ports.

If a CAIS/LAIS houses more than one DARU, the units are multi-dropped together. One DARU is always linked to the ARCs (either directly or by modems and telephone lines) so that the announcement vocabulary can be downloaded from the ARCs if necessary.

:=:

Much of the information in this file is copied verbatim from the instructional booklet sent to me by CCI. Their documentation is extremely in-depth and well written, and, with some looking over, is easy to understand. Much of the information in here is confusing with all of the acronyms used as well as technical terms, but if you cross-reference acronyms throughout the file, you should be able to see what it stands for. Also, if you don't understand what something does, just think of it in terms of use by the telephone company in the context used and you can generally get an idea of what it does or is used for. I hope you enjoyed this file and continue to read Phrack Inc. files to learn more about the system we use and experience. Any constructive suggestions are welcomed directly or indirectly.

Taran King

:=:
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

==Phrack Inc.==

Volume Two, Issue Eleven, Phile #7 of 12

```
-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-
!                                               !
#     Hacking Primos I, II, III                 #
!                                               !
#           (I&II  Revised)                     #
!                                               !
#             By Evil Jay                       #
!                                               !
-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-
```

Author Note:

Ugg! I looked at my first file after it was released and saw a lot of misspellings, errors and other screw-ups and was completely embarrassed. I did not have time to edit the file and I was also writing the second file which dealt with gaining privileges. I threw these two files at Taran King who in turn merged them together. So I humbly apologize for all of the errors in the last file. In this file I will revise the old file and continue with some more methods of gaining access and also list out some very basic commands for beginners. As I said before, if you have any questions you can reach me on any board I am currently inhabiting. Hope to hear from you...

*** Gaining Access From Scratch ***

I made a mistake in my last file and stated that FAM was not a default. FAM is a default, but it can be taken out by the system administrators.

To get a listing of every possible account on a system, it is really quite easy. They are located in the MFD directories. Type:

A MFD <MFD #> (Without the "<" and ">" signs)

Or just:

A MFD

Then type LD and hit return. Now, you will see a listing of files and underneath should be a listing of directories appropriately named Directories. These directories are valid User IDs. However, I believe that directories that have an "*" character in them cannot be logged in to.

*** Getting Higher Access Revised ***

SYS1 is the highest system level there is. Meaning unless commands have to be entered from the supervisors terminal, you can usually do anything with an account that has SYS1 access. Also, I should clarify that SYS1 will not always be the name of the highest access available. It could be named SYSTEM or anything for that matter.

You are looking for a file with the extension .CPL - look for this file under any of the SYS1 directories. When you find one, SLIST it. You are looking for a line similar to:

A <DIRECTORY NAME> <PASSWORD>

It could look like:

A LIB XXX

LIB is the directory (user id) name.

XXX is the password to that directory (user id).

When you have this, log into that account with the directory name and password. If your lucky you'll gain access to that account. I have noticed that a lot of high access accounts sometimes have the password XXXXXX or X. Try these, I am unsure as to whether they are actual defaults or not.

Ah, the revision is done! Now some more ways to gain access...

*** The Trojan Horse ***

Providing you have access, you may or may not be able to edit a file in a high access directory. If you can't then try the above technique and try to hack a higher level account.

You will first want to learn the Command Processing Language (CPL). Type HELP CPL for a list of commands and then play around and try to write your own programs. If you don't have a manual handy, look at other CPL programs in other directories you can access. Once you know CPL, all you have to do is edit a CPL file in a high access dir. Add your own high level commands to the program. Then replace the old file, logoff and wait until the operator(s) decide to run your program. Hopefully, if everything goes well your routines will help you with whatever you wanted. However it would be a good idea to have your TH write a file to your directory telling you whether it has been ran or not. I will discuss different Trojan Horses in later issues of Phrack.

Once on a Prime it is pretty easy to get other accounts so don't worry about it. Just worry about getting on in the first place. Patience is definitely required since many systems (particularly versions 19 up) tend to hang up after the first invalid id/password combo.

*** Basic Commands For Beginners ***

This is a list of basic commands you can use once on a Prime system. I will not go in-depth on a command, because you can do that for yourself by typing:

HELP <COMMAND NAME>

SLIST <FILENAME>

This will list out the contents of a file on a directory. Type in the full file name (plus extension).

ATTACH <DIRECTORY NAME>

This will attach you to another directory. For a full explanation type HELP ATTACH.

LD

This will list all the files and subdirectories in a directory.

RLS -ALL

Commands add up on the stack, and eventually after a pre-determined amount of commands you will get a message telling you that you are "now at command level

XX". This command will release all those pent up commands in the stack.

CPL <FILENAME>

This will run a file with the extension ".CPL".

COMINPUT <FILENAME>

This will run a file with the extension ".COM"

SEG <FILENAME>

This will run a file with the extension ".SEG"

STATUS USERS

This will give you a listing of users and other information currently on the system.

STATUS

This will give you the status of the system and other information.

EDIT (Or ED)

This is a text editor.

CHANGE_PASSWORD <OLD PASSWORD>

Does just what it says it does.

DELETE <FILENAME>

Deletes a file.

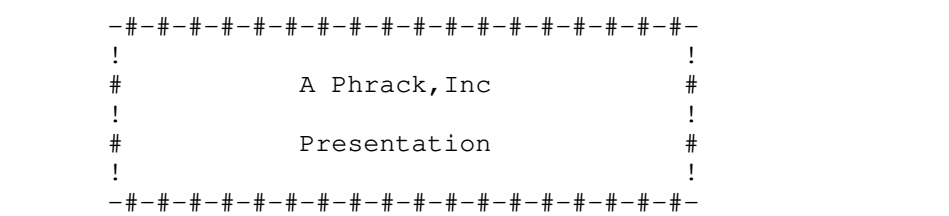
LOGOFF

I think this is pretty obvious.

LOGIN

This will log you out and take you back to the login process, providing there is no logins-over-logins set by the administrators.

This is a very small list, but will probably help the beginner greatly when he/she first logs on. Hope you enjoyed this issue...Look for Hacking Primos Part IV in Phrack, 12. Mebbe'.



==========

==Phrack Inc.==

Volume Two, Issue Eleven, Phile #8 of 12

Telephone Signalling Methods

Written by Doom Prophet

This file explains the basic signalling methods in use by the telephone system and is intended for general understanding. The text that follows is not highly technical since this file is for basic understanding and aimed at less experienced phreaks. Still, the more experienced readers may want to read it as a review on the information.

Analog--Analog signals are those that have continuously and smoothly varying amplitude or frequency. Speech signals are of this type when you consider tone, pitch and volume levels that vary according to the person speaking. When a person speaks into the transmitter on a telephone, the voice signals are made up of acoustical energy, which are then converted into electrical energy for transmission along a transmission medium.

Analog carrier facilities may operate over different media, such as wire lines, multi-wire cable, coaxial cable, or fiber optic cable. Copper wire is the most commonly used for subscriber loops.

A technique that allows for many signals to be sent along the same transmission path is called Multiplexing. Analog signals use Frequency Division Multiplexing or FDM.

Digital--Instead of the voice signal being processed as an analog signal, it is converted into a digital signal and handled with digital circuits throughout the transmission process. When it arrives at the CO that serves the called telephone, it is converted back to analog to reproduce the original voice transmission.

Pulse Code Modulation or PCM is when the binary signal is transmitted in serial form. Binary coding represents bits or binary digits at 0 and 1 levels. These levels have a definite time relationship with one another. Time Division Multiplexing or TDM is the type of multiplexing, sometimes abbreviated as MUX, done for digital transmission.

Metallic--Metallic facilities carry only one Voice Frequency (VF) channel. Typically, a metallic facility is used to connect business or residential lines to a CO. Coaxial cable can be used to transmit both Analog and Digital signals as well as Metallic signals.

VF channels have a 4000 Hz bandwidth, from 0 to 4000 Hz. However, the in-band range of the voice frequency is between 200 and 3400 Hz. Signals that are out of this frequency range but still within the VF channel are out of band signals. A supervisory equivalent to 2600 for out of band is 3700 Hz. The amount of VF channels vary according to the transmission facilities that are being used.

CCIS (Common Channel Interoffice Signalling) is where control or supervisory signals are sent on a separate data link between switching offices. CCIS links operate at 4800 bps, or baud. Signal Transfer Points in the switch send the supervisory information over the dedicated link. This prevents supervisory tones from subscriber stations to register with the telephone network as a change in trunk status.

Reverse Battery Signalling- When the called end answers, the polarity and condition of the Ring and Tip leads is reversed to indicate the status of the connection. Conditions for a call being placed, but not yet answered, is ground on the Tip and battery (the CO battery current is flowing through) on the Ring. When the called party answers, by the action of relays in the switching equipment, current is reversed in the calling subscriber loop and battery is placed on the Tip and ground on the Ring, which remains during the talking.

E and M- Leads connecting switching equipment to trunk circuits are termed the E and M leads, for receive and transmit. The E lead reflects the far-end or terminating end condition of the trunk. Ground on the E lead indicates that a signal has been received from the other end. The E lead is open when the trunk is idle. The M lead reflects the the near end condition of the trunk. It is grounded when the trunk is idle, and goes to battery condition when the called party goes off hook. Long interoffice and short haul toll trunks use this signalling method.

It should be noted that AC signalling is Alternating Current, and is used on the intertoll network, and interoffice and short haul toll trunks. DC, or direct current, is used on two wire or intraoffice connections, and local interoffice trunks.

Single Frequency (SF)- Single Frequency is an in-band 2600 Hz signalling system. When a four wire trunk is idle, and is equipped for SF in band signalling, a 2600 Hz tone is being transmitted in both directions. When the trunk is seized at an originating position, the M lead is changed from ground to battery state. This removes the 2600 Hz supervisory tone from the outgoing trunk pair. The loss of the 2600 Hz will be detected at the far end by the SF signalling unit, changing the far end E lead condition from open to ground, causing switching equipment to function. When ground is restored to the M lead, replacing 2600 on the near end trunk, the pulsing of address information begins.

Multi-Frequency (MF)- The MF pulsing method uses AC signals in the voice frequency range, and transmits address information between COs by combinations of only 2 of 5 frequencies. MF is used for the sending of address information, as mentioned before. Other signalling methods are still required for trunk control and supervision. There are six MFs comprising MF codes. These are 200 Hz apart in the 700-1700 range. Two frequencies are sent at once, thus explaining the term 'Multi frequency.'

MF pulsing is initiated by manual keysets and the TSPS switchboard, or by MF outpulsing senders in ESS and Xbar. MF pulsing is very rapid and only occurs when a connection is being established. KPs, or Key Pulses, are used as a signal to start MF pulsing. STs, or STart tones are used as a signal to indicate the end of MF pulsing.

As an example of MF signalling, take a toll switchboard trunk connected to a Xbar Central Office. The operator selects an idle trunk, and presses the KP button on the keyset to signal the distant sender or register link equipment to connect to a MF receiver. The S lamp on the keyset will light when the far end is ready to receive MF pulses. After keypulsing the digits of the called number, the operator presses the ST button, which indicates the end of pulsing and disconnects the keyset from the operator's cord circuit and extinguishes the KP and S lamps.

At the terminating CO, the two MF tones of each digit are amplified and limited in the MF receiver unit associated with the incoming sender and register circuit. The frequencies are selected by channel filters in the MF receiver and then detected. The DC voltage that results will operate the proper channel relays to continue with the process of placing the call.

==Phrack Inc.==

Volume Two, Issue Eleven, Phile #9 of 12

The following is reprinted from the November 1985 issue of Personal Communications Technology magazine by permission of the authors and the publisher, FutureComm Publications Inc., 4005 Williamsburg Ct., Fairfax, VA 22032, 703/352-1200.

THE ELECTRONIC SERIAL NUMBER: A CELLULAR 'SIEVE'? 'SPOOFERS' CAN DEFRAUD USERS AND CARRIERS

by Geoffrey S. Goodfellow, Robert N. Jesse, and Andrew H. Lamothe, Jr.

What's the greatest security problem with cellular phones? Is it privacy of communications? No.

Although privacy is a concern, it will pale beside an even greater problem: spoofing.

'Spoofing' is the process through which an agent (the 'spoofer') pretends to be somebody he isn't by proffering false identification, usually with intent to defraud. This deception, which cannot be protected against using the current U.S. cellular standards, has the potential to create a serious problem--unless the industry takes steps to correct some loopholes in the present cellular standards.

Compared to spoofing, the common security concern of privacy is not so severe. Most cellular subscribers would, at worst, be irked by having their conversational privacy violated. A smaller number of users might actually suffer business or personal harm if their confidential exchanges were compromised. For them, voice encryption equipment is becoming increasingly available if they are willing to pay the price for it.

Thus, even though technology is available now to prevent an interloper from overhearing sensitive conversations, cellular systems cannot--at any cost--prevent pirates from charging calls to any account. This predicament is not new to the industry. Even though cellular provides a modern, sophisticated quality mobile communications service, it is not fundamentally much safer than older forms of mobile telephony.

History of Spoofing Vulnerability

The earliest form of mobile telephony, unsquelched manual Mobile Telephone Service (MTS), was vulnerable to interception and eavesdropping. To place a call, the user listened for a free channel. When he found one, he would key his microphone to ask for service: 'Operator, this is Mobile 1234; may I please have 555-7890.' The operator knew to submit a billing ticket for account number 1234 to pay for the call. So did anybody else listening to the channel--hence the potential for spoofing and fraud.

Squelched channel MTS hid the problem only slightly because users ordinarily didn't overhear channels being used by other parties. Fraud was still easy for those who turned off the squelch long enough to overhear account numbers.

Direct-dial mobile telephone services such as Improved Mobile Telephone Service (IMTS) obscured the problem a bit more because subscriber identification was made automatically rather than by spoken exchange between caller and operator. Each time a user originated a call, the mobile telephone transmitted its identification number to the serving base station using some form of Audio Frequency Shift Keying (AFSK), which was not so easy for eavesdroppers to understand.

Committing fraud under IMTS required modification of the mobile--restrapping

of jumpers in the radio unit, or operating magic keyboard combinations in later units--to reprogram the unit to transmit an unauthorized identification number. Some mobile control heads even had convenient thumb wheel switches installed on them to facilitate easy and frequent ANI (Automatic Number Identification) changes.

Cellular Evolution

Cellular has evolved considerably from these previous systems. Signaling between mobile and base stations uses high-speed digital techniques and involves many different types of digital messages. As before, the cellular phone contains its own Mobile Identification Number (MIN), which is programmed by the seller or service shop and can be changed when, for example, the phones sold to a new user. In addition, the U.S. cellular standard incorporates a second number, the 'Electronic Serial Number' (ESN), which is intended to uniquely and permanently identify the mobile unit.

According to the Electronic Industries Association (EIA) Interim Standard IS-3-B, Cellular System Mobile Station--Land Station Compatibility Specification (July 1984), 'The serial number is a 32-bit binary number that uniquely identifies a mobile station to any cellular system. It must be factory-set and not readily alterable in the field. The circuitry that provides the serial number must be isolated from fraudulent contact and tampering. Attempts to change the serial number circuitry should render the mobile station inoperative.'

The ESN was intended to solve two problems the industry observed with its older systems.

First, the number of subscribers that older systems could support fell far short of the demand in some areas, leading groups of users to share a single mobile number (fraudulently) by setting several phones to send the same identification. Carriers lost individual user accountability and their means of predicting and controlling traffic on their systems.

Second, systems had no way of automatically detecting use of stolen equipment because thieves could easily change the transmitted identification.

In theory, the required properties of the ESN allow cellular systems to check to ensure that only the correctly registered unit uses a particular MIN, and the ESNs of stolen units can be permanently denied service ('hot-listed'). This measure is an improvement over the older systems, but vulnerabilities remain.

Ease of ESN Tampering

Although the concept of the unalterable ESN is laudable in theory, weaknesses are apparent in practice. Many cellular phones are not constructed so that 'attempts to change the serial number circuitry renders the mobile station inoperative.' We have personally witnessed the trivial swapping of one ESN chip for another in a unit that functioned flawlessly after the switch was made.

Where can ESN chips be obtained to perform such a swap? We know of one recent case in the Washington, D.C. area in which an ESN was 'bought' from a local service shop employee in exchange for one-half gram of cocaine. Making the matter simpler, most manufacturers are using industry standard Read-Only Memory (ROM) chips for their ESNs, which are easily bought and programmed or copied.

Similarly, in the spirit of research, a west coast cellular carrier copied the ESN from one manufacturer's unit to another one of the same type and model--thus creating two units with the exact same identity.

The ESN Bulletin Board

For many phones, ESN chips are easy to obtain, program, and install. How does a potential bootlegger know which numbers to use? Remember that to obtain service from a system, a cellular unit must transmit a valid MIN (telephone number) and (usually) the corresponding serial number stored in the cellular

switch's database.

With the right equipment, the ESN/MIN pair can be read right off the air because the mobile transmits it each time it originates a call. Service shops can capture this information using test gear that automatically receives and decodes the reverse, or mobile-to-base, channels.

Service shops keep ESN/MIN records on file for units they have sold or serviced, and the carriers also have these data on all of their subscribers. Unscrupulous employees could compromise the security of their customers' telephones.

In many ways, we predict that 'trade' in compromised ESN/MIN pairs will resemble what currently transpires in the long distance telephone business with AT&T credit card numbers and alternate long-distance carrier (such as MCI, Sprint and Alltel) account codes. Code numbers are swapped among friends, published on computer 'bulletin boards' and trafficked by career criminal enterprises.

Users whose accounts are being defrauded might--or might not--eventually notice higher-than-expected bills and be reassigned new numbers when they complain to the carrier. Just as in the long distance business, however, this number 'turnover' (deactivation) won't happen quickly enough to make abuse unprofitable. Catching pirates in the act will be even tougher than it is in the wireline telephone industry because of the inherent mobility of mobile radio.

Automating Fraud

Computer hobbyists and electronics enthusiasts are clever people. Why should a cellular service thief 'burn ROMs' and muck with hardware just to install new IDs in his radio? No Herculean technology is required to 'hack' a phone to allow ESN/MIN programming from a keyboard, much like the IMTS phone thumb wheel switches described above.

Those not so technically inclined may be able to turn to mail-order entrepreneurs who will offer modification kits for cellular fraud, much as some now sell telephone toll fraud equipment and pay-TV decoders.

At least one manufacturer is already offering units with keyboard-programmable MINs. While intended only for the convenience of dealers and service shops, and thus not described in customer documentation, knowledgeable and/or determined end users will likely learn the incantations required to operate the feature. Of course this does not permit ESN modification, but easy MIN reprogrammability alone creates a tremendous liability in today's roaming environment.

The Rolls Royce of this iniquitous pastime might be a 'Cellular Cache-Box.' It would monitor reverse setup channels and snarf ESN/MIN pairs off the air, keeping a list in memory. Its owner could place calls as on any other cellphone. The Cache-Box would automatically select an ESN/MIN pair from its catalog, use it once and then discard it, thus distributing its fraud over many accounts. Neither customer nor service provider is likely to detect the abuse, much less catch the perpetrator.

As the history of the computer industry shows, it is not far-fetched to predict explosive growth in telecommunications and cellular that will bring equipment prices within reach of many experimenters. Already we have seen the appearance of first-generation cellular phones on the used market, and new units can be purchased for well under $1000 in many markets.

How High The Loss?

Subscribers who incur fraudulent charges on their bills certainly can't be expected to pay them. How much will fraud cost the carrier? If the charge is for home-system airtime only, the marginal cost to the carrier of providing that service is not as high as if toll charges are involved. In the case of toll charges, the carrier suffers a direct cash loss. The situation is at its worst when the spoofer pretends to be a roaming user. Most inter-carrier roaming agreements to date make the user's home carrier (real or spoofed)

responsible for charges, who would then be out hard cash for toll and airtime charges.

We have not attempted to predict the dollar losses this chicanery might generate because there isn't enough factual information information for anyone to guess responsibly. Examination of current estimates of long-distance-toll fraud should convince the skeptic.

Solutions

The problems we have described are basically of two types. First, the ESN circuitry in most current mobiles is not tamper-resistant, much less tamper-proof. Second and more importantly, the determined perpetrator has complete access to all information necessary for spoofing by listening to the radio emissions from valid mobiles because the identification information (ESN/MIN) is not encrypted and remains the same with each transmission.

Manufacturers can mitigate the first problem by constructing mobiles that more realistically conform to the EIA requirements quoted above. The second problem is not beyond solution with current technology, either. Well-known encryption techniques would allow mobiles to identify themselves to the serving cellular system without transmitting the same digital bit stream each time. Under this arrangement, an interloper receiving one transmission could not just retransmit the same pattern and have it work a second time.

An ancillary benefit of encryption is that it would reasonably protect communications intelligence--the digital portion of each transaction that identifies who is calling whom when.

The drawback to any such solution is that it requires some re-engineering in the Mobile-Land Station Compatibility Specification, and thus new software or hardware for both mobiles and base stations. The complex logistics of establishing a new standard, implementing it, and retrofitting as much of the current hardware as possible certainly presents a tough obstacle, complicated by the need to continue supporting the non-encrypted protocol during a transition period, possibly forever.

The necessity of solving the problem will, however, become apparent. While we presently know of no documented cases of cellular fraud, the vulnerability of the current standards and experience with similar technologies lead us to conclude that it is inevitable. Failure to take decisive steps promptly will expose the industry to a far more expensive dilemma. XXX

Geoffrey S. Goodfellow is a member of the senior research staff in the Computer Science Laboratory at SRI International, 333 Ravenswood Ave., Menlo Park, CA 94025, 415/859-3098. He is a specialist in computer security and networking technology and is an active participant in cellular industry standardization activities. He has provided Congressional testimony on telecommunications security and privacy issues and has co-authored a book on the computer 'hacking' culture.

Robert N. Jesse (2221 Saint Paul St., Baltimore, MD 21218, 301/243-8133) is an independent consultant with expertise in security and privacy, computer operating systems, telecommunications and technology management. He is an active participant in cellular standardization efforts. He was previously a member of the senior staff at The Johns Hopkins University, after he obtained his BES/EE from Johns Hopkins.

Andrew H. Lamothe, Jr. is executive vice-president of engineering at Cellular Radio Corporation, 8619 Westwood Center Dr., Vienna, VA 22180, 703/893-2680. He has played a leading role internationally in cellular technology development. He was with Motorola for 10 years prior to joining American TeleServices, where he designed and engineered the Baltimore/Washington market trial system now operated by Cellular One.

A later note indicates that one carrier may be losing something like $180K per month....