==Phrack Inc.==

Volume Two, Issue Ten, Phile #1 of 9

1/1/87

Introduction...

Well, we have made it to this, the start of a new year and the start of a new volume of Phrack Inc. This has taken quite a while to get the long awaited issue out, and it's been procrastinated quite a bit, so I apologize to those that have been patiently waiting. We have purposely waited a bit, but we also are releasing this Phrack approximately at the same time as the Legion of Doom/Hackers Technical Journal, which is another high quality newsletter working with us rather than against us, and I personally recommend the documents as highly informative. I really enjoyed it and hope you continue to support both of us.

If you wish to write for Phrack Inc., merely get in touch with myself, Knight Lightning, Cheap Shades or Beer Wolf or anyone that knows us or is on any of the MSP boards and we shall either get back to you or get in contact with you in some manner. File topics can be either telecommunications or on operating systems or some unique aspect/flaw of security. Be looking forward to more Phrack issues in the near and far future. Later
-TK

This issue of Phrack Inc. includes the following:

~~~~~~
~~~~~~

==Phrack Inc.=

Volume Two, Issue 10, Phile #2 of 9

==Phrack Pro-Phile 7==

Written and Created by Taran King

12/15/86

Welcome to Phrack Pro-Phile 7. 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 user from the golden years of hacking and phreaking...

Dave Starr
~~~~ ~~~~~

Dave is one of the old phreakers and hackers that accomplished so much through voice phreaking and literal hacking rather than reading others' findings to learn. A master engineer, voice phreaking is one unto itself. Dave has a PhD in B.S.

```
-------------------------------------------------------------------------------
-
Personal
~~~~~~~~
             Handle: Dave Starr
           Call him: Dave Starr
       Past handles: Micronet Phantom and Big Brother
      Handle origin: Micronet Phantom came from working with The Source
                     computer and Big Brother, of course, came from George
                     Orwell's 1984.
      Date of Birth: 5/6/62
Age at current date: 24
             Height: 6' 0"
             Weight: 170 lbs.
          Eye color: Brown
         Hair Color: Light Brown
          Computers: TRS-80 (4k version), Apple ][, ][+, ][e
  Sysop/Co-Sysop of: Starcom Network

-------------------------------------------------------------------------------
-
```

Dave started out on The Source, and stuck with them for 6 to 8 months hacking around the system because the system was so slow security-wise, and of course, from there, he got involved with hacking Primes. One of the security agents named Paul from Dialcom got in contact with Dave and discussed Dave's hacking on The Source (his system). After talking, they found they had common interests, which included hacking and phreaking. Paul gave Dave his first code to a local dial-up for Sprint. He also led him in the direction of 8BBS, which brought him to meet the best of the nation's phreakers and hackers at the time, which included Susan Thunder, Roscoe DuPran, and Kevin Mitnick. Susan and Roscoe were strong friends of Dave that he personally met as well as Kevin, but he never met Kevin. He met Susan in the L.A. County Courthouse testifying against her, with Susan and Roscoe using these handles as real names on the charges of harassment. The phreak/hack BBS's that were most memorable for Dave were 8BBS and his own, Starcom Network, which had hidden commands for accessing the phreak section. Starcom Network was a nationally networked system that Dave created and operated. This was a virtual copy of The Source, for which he went to court over. They claimed it was their system, but he supressed them with a threat of publicity. Modem Over
```

Manhattan was another memorable board on a TRS-80. He attributes his phreak knowledge to Paul from Dialcom and to The Source for his hacking ability as well as Susan Thunder for information on RSTS.

Dave Starr does intelligence and counter-intelligence work for anyone who has money and who is not against the United States or the views of the United States.

Dave has always operated independently, never being a member of a club or group, and has hand-picked his partners.

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

Interests: Telecomputing (phreaking and hacking), movies, a fascination with the match-making systems (Dial-Your-Match type systems), fun, video components.

## Dave's Favorite Things

Women: A quiet evening with the girlfriends (NOTE: Plural).
Cars: Mercedes 450-SL (his girlfriend's).
Foods: Italian.
Music: Anything excluding acid rock/heavy metal.
Leisure: Smoking, but he hates cigarettes.

## Most Memorable Experiences

Bringing The Source's system to their knees.
The Source hackers made demands of a rate of reduction to a minimum of a 33% decrease, which was sent with the comment, "I am in business so I understand the money, but you are becoming too fucking greedy." Also, an article in Source-World magazine was demanded, bigger than the one in the last issue which was to contain the following: how long they'd been on the Source, why they were doing this, The Source's demented point of view, their correct point of view, how long they have been terrorizing the Source, and an apology for lying to all the users that the rate increase was necessary, AND an open apology to The Pirate and Micronet Phantom saying sorry for all the trouble The Source had caused them in their quest for fair and free Sourcing. They wanted 2 seclev 4 accounts (normal is 3). They assured The Source that they could get them here for free, and low-and-behold, they could create anything, but they didn't want the harassment. If they did get harassed, they would immediately log in under seclev 7 and kill the system. The threatened that various accounts would be killed (all with seclev 4 and up). The Source person wrote, "Was this ever answered?". They then went on to say that they wouldn't do any more terrorizing provided that it was responded to their acct. within 20 minutes.
For deleting an account, he sent back a message saying, "Fuck you". He explained how they were powerless against The Pirate and Micronet Phantom, and how The Source shouldn't even try to catch them. They were to continue to attack "The Empire" (The Source) until it was fair for the users.
Numerous other letters that played to the same tune.

## Some People to Mention

TCA Vic of The Source - Customer Service Manager/Gestapo Police
(Who he dearly hated and always has thought of sticking a broomstick up his ass)

Paul of Dialcom (Introduced him to phreaking and put his paranoia to rest)
Susan Thunder (For teaching him RSTS and other things)
Bruce Patton (On his rag list due to a disagreement.  He received a electricity shut-down and a phone system shut-down of his law office as well as forwarding all calls to the 8BBS)
Roscoe DuPran (For having him go to court with him and meeting Susan in person and for many other things [unmentionable here])
The Pirate of Las Vegas (For his helpful continual harassment of The Source)
Kevin Metnick (For his infrequent but helpful service)
Larry of Modem Over Manhattan (For being there and his BBS being there)
Bernard of 8BBS (For being there and his BBS being there)

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

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

Of the general population of phreaks you have met, would you consider most phreaks, if any, to be computer geeks?  Only The Pirate, a 13 year old, fit this description.  Thank you for your time, Dave.

Taran King
Sysop of Metal Shop Private

==Phrack Inc.==

Volume Two, Issue Ten, Phile #3 of 9

```
*********************************
*         The TMC Primer        *
*-------------------------------*
*     Written by: Cap'n Crax    *
*-------------------------------*
*        December 17, 1986      *
*********************************
```

This file was originally intended to be a "data file" of info on TMC ports, formulas, etc, but I decided that it would serve a better use as a "tutorial" of sorts. But first a bit of background info...

Who is TMC?

TMC (TeleMarketing Communications) is a long distance service serving all 50 states. While not as well known as MCI or Sprint, they are a fairly large company. They are capable of setting up business communications systems, PBX's, and residential service. Unlike most LDC's, however, they operate on a "franchise" basis, which means that each franchise of the company has little information about any other franchise, although they do use the same lines and the same type of equipment.

So, what can they do for me?

Well, for most of us, TMC offers many new potentials for abuse. One of the primary weak points of the company is the code formats that they decided to use. Codes on all TMC ports are seven digits. If they were generated randomly, this would be a reasonably secure system from sequential code hacking. But TMC doesn't use random codes. Instead, they use a checksum based formula system, with different formulas on each port. I assume that this is because they wanted a wide displacement of the codes over the seven-digit series, so that a sequential code hacker wouldn't be able to get 2 or 3 good codes in a row. Or perhaps they are just very stupid. In any case, it's interesting that they seem to have never thought of what could happen if anyone ever managed to figure out any of these formulas. Anyway, that's what this file is about.

Great! What else can you tell me?

Well, TMC seems to use some form of the Dimension PBX system for their billing system (Their ads say that the switching equipment is digital). This makes TMC ports easily identifiable by the "Hi-Lo" bad code siren. For those who worry about such things, TMC is one of the "safer" companies to use. This is largely because, unlike "unified" companies like MCI, TMC franchises don't really care if another franchise is losing money. Since each franchise is independent of all others, there are many 800 ports, one for each franchise. If you use an out-of-state 800 port, you are free from such worries as ANI, which I have never perceived as a major threat to the code-user anyway. Also, TMC offers lots of opportunities for the aspiring security consultant (hehehe).

Ok, so where's some real info?

Right here. I am going to explain as much about TMC hacking as I can manage, without actually handing out codes. First, an example port. The example I am using is the 800 port for Louisville, KY.

1-800-626-9600

This is the port. If you are not familiar with TMC, you may want to call it to see what it sounds like. So let's say you call it and recognize it as a TMC. What next? Well, a good bet would be to run a standard "code-hack" program on it... Set it for seven digits, 1+ the number, and note that TMC codes start with 0 on more than 50% of the ports I have seen. So let's say that you then get this list of (fictional) codes...

0347589
0347889
0348179
0350358
0355408

At first glance, this may look like a series of "random" numbers. But, look closer. These numbers are based on a checksum. It is as follows...

Code Format: 03xabcy
x+y=13
(In the first code, x=4 and y=9, and, of course, 4+9=13)
a+c=15
(Here, a=7 and c=8, and 7+8=15)
b=1 to 9
(Digit "b" is unrelated to the rest of the numbers. It could, for example, be varied from 1-9 to possibly find more working codes)

Also note that 0+5 would equal 15, since the 0 is really a 10. Really!

Please note that the above formula is only fictional. I wouldn't want to possibly cause loss to TMC by giving away codes on their system!

Is that all?

No, of course not. TMC, in their love of telecom enthusiasts, has also put an additional prize in the Krackerjack box. The vast majority of TMC ports have "Outside Line" codes, which is a 2 or 3 digit number, that, when entered after certain codes, will give an AT&T dialtone. This is apparently a holdover from the fact that they are using PBX equipment. Anyway, if anyone is asking why you'd want an AT&T dialtone, (does anyone need to ask?) it will allow unrestricted calling. This, of course, means 976's, 900's, Alliance Teleconf., international calling, etc... Naturally, I can't list any of these, but I can say that if it is 2 digits, it would start with any number from 2-9 and end in 8 or 9. If it is three digits, it will almost always start with 6, and be followed by any two digits. Some possible outside line codes would be 59, 69, 89, 99, 626, 636, 628, etc... These, of course, are only examples of possible codes. As I mentioned, these O/S line codes are entered after the seven digit code. The O/S line codes only work after certain 7-digit codes, and from my experience, the 7-digit codes that they work with normally can't be used for the usual 7 digits+1+number dialing. I can find no apparent pattern to the codes that they do work with, so you will have to find them by trial-and-error.

What, you want more?

Ok, well, here's a few 800 ports...

1-800-433-1440
1-800-354-9379
1-800-227-0073
1-800-248-4200
1-800-331-9922
1-800-531-5084
1-800-451-2300
1-800-351-9800

Closing.

Please note that this article is only intended as an overview of TMC and why they would/wouldn't be a good choice for your long distance needs. And goodness me, don't use any of this information in an illegal way!

==Phrack Inc.==

Volume Two, Issue Ten, Phile #4 of 9

A Beginner's Guide to:
The IBM VM/370
(or what to do once you've gotten in)

A monograph by Elric of Imrryr
Presented by Lunatic Labs UnLimted.

Note: This file is formatted for printing
on a 80 Column, 55 line printer.

PREFACE: What this guide is about.

This was written to help Hackers learn to basics of how to function on an IBM VM/370. Not as a guide on how to get in, but on how to use it one you have gotten in.

Comments on this are welcome at RIPCO 312-528-5020.

Note: To VM/370 Hackers, feel free to add to this file, just give myself & Lunatic Labs credit for our parts.

PART 1: Logging in & out

When you connect to a VM/370 system hit RETURN till you see:

```
VM/370
!
```

To logon you type:

```
logon userid ('logon' may be abbreviated to 'l')
```

If you enter an invalid userid, It will respond with a message:
'userid not in cp directory'.
If it is valid you with get:

```
ENTER PASSWORD:
```

Enter your password, then your in, hopefully....

Logging Out:
Type:

```
log
```

PART 2: Loading CMS & Getting set up

When you logon, if you do not see the message 'VM/SP CMS - (date) (time)
you will need to load 'CMS' (CMS in a command interpreter).
Type:

```
cp ipl cms
```

You should then see something like this:

```
R; T=0.01/0.01 08:05:50
```

Now you will be able to use both CP & CMS commands...
Some system my think you are using an IBM 3270 Terminal, if you can
emulate a 3270 (for example with Crosstalk) do so, if not type:

```
set terminal typewriter or set terminal dumb
```

PART 3: Files

You can list your files by typing:

```
filelist
```

Wildcards can be used, so:

```
filelist t*
```

list all files beginning with a 't'.
Filenames are made up of a FILENAME and FILETYPE

You can list a file by typing:

```
listfile filename filetype
```

Other file commands are: copyfile, erase, and rename, they all work with FILENAME FILETYPE.

PART 4: Editing your files

I'm going to keep this down to the basics and only discuss one editor XEDIT. To use XEDIT type:

```
xedit filename filetype
```

Once in XEDIT, enter the command 'input' to enter text, hit a RETURN on a blank line to return to command mode, then enter the command 'FILE' to save your file.

PART 5: Communicating with others on the system

Sending & receiving 'NOTES':
To send a 'NOTE' to another user type:

```
note userid
```

You will then be in the XEDIT subsystem, see PART 4.
Once you are done writing your NOTE, save the file and type:

```
send note
```

This will send the NOTE to userid.
You can also use the SEND command to send other files by typing:

```
send filename filetype userid.
```

Sending messages:
You can use the TELL command to communicate with a user who is current logged on, type:

```
tell userid Help me!
```

PART 6: Getting Help

Type:

```
help
```

That's it, good luck.

```
                               ==Phrack Inc.==

                     Volume Two, Issue Ten, Phile #5 of 9

                 ^                                         ^
               [<+>]                                     [<+>]
               /|-|\                                     /|-|\
               \|P|/>/>/>/>/>/>/>/>/>PLP<\<\<\<\<\<\<\<\<\|P|/
                |h|           ^                 ^         |h|
                |a|          ]+[The Executioner]+[        |a|
                |n|                                       |n|
                |t|      Call Phreak Klass, Room 2600     |t|
                |o|            [806][799][0016]           |o|
                |m|                                       |m|
                |s| [Circuit Switched Digital Capability] |s|
                |-|  -----------------------------------  |-|
                |S|                                       |S|
                |e|  Part I of II in this series of files |e|
                |x|                                       |x|
                |y|      Written for PHRACK, Issue 10.    |y|
               /|-|\                                     /|-|\
               \|$|/>/>/>/>/>/>/>/>/>PLP<\<\<\<\<\<\<\<\<\|$|/
               [<+>]                                     [<+>]
```

========
=Part I=
========

The Circuit Switch Digital Capability (CSDC) allows for the end to end digital transmission of 56 kilobits per second (kb/s) data and, alternately, the transmission of analog voice signals on a circuit switched basis.

=====================
=Network Perspective=
=====================

The CSDC feature was formerly known as PSDC (Public Switched Digital Capability). These two terms can be used synonymously. The CSDC feature provides an alternate voice/data capability. If a SLC Carrier System 96 is used, digital signals are transmitted by T1 signal. If the loop is a two wire loop, the CSDC feature utilizes time compression multi-plexing (TCM) which allows for the transmission of digital signals over a common path using a separate time interval for each direction. During a CSDC call an end user may alternate between the voice and data modes as many times as desired. The CSDC feature can support sub-variable data rates from customer premises equipment, but a 56 kb/s rate is utilized in the network. Some possible applications of the CSDC feature are:

1. Audiographic Teleconferencing.
2. Secure Voice.
3. Facsimile.
4. Bulk Data.
5. Slow scan television.

The ESS switch provides end user access and performs signalling, switching, and trunking functions between the serving ESS switch and other CSDC offices. End users of CSDC require a network channel terminating equipment circuit (NCTE) which is the SD-3C476 or its equivalent. End user access is over 2-wire metallic loops terminating at the metallic facility terminal (MFT) or SLC

Carrier System. End users not served directly by a direct CSDC ESS office, can access CSDC equipment through a RX (Remote Exchange) access arrangement via use of a D4 Carrier System and if required, a SLC Carrier System. The T-Carrier trunks serve for short haul transmissions while long haul transmissions are served by digital microwave radio and other digital systems.

If the NCTE interface is used with customer premises equipment, a miniature 8-position series jack is used to connect the NCTE to other equipment. The jack pins are paired off; data transmit pair, data receive pair, a voice pair, and a mode switch pair. The data pairs support the simultaneous transmission and reception of digital data in a bipolar format at 56 kb/s. The data pairs also provide for the xmission of control information to and from the network. The voice pairs supports analog signal transmission and provides for call setup, disconnect and ringing functions. The mode control pair provides signals to the network when a change in mode (voice to data/data to voice) is requested by the customer.

A CSDC call is originated over a 2-wire loop which can also be used for Message Telecommunication Service (MTS) calls. Lines may be marked (MTS/CSDC or CSDC only). Touch tone is needed to originate a CSDC call. Originations may be initiated manually or with Automatic Calling Equipment (ACE) if available. Digit reception, transmission and signalling follow the same procedures used for a MTS outgoing call on CCIS or non-CCIS trunks. However CSDC calls are ALWAYS routed over digital transmission facilities.

The long term plan also allows for EA-MF (Equal Access-Multi Frequency) signalling and improved automatic message accounting (AMA) records. A CSDC call is screened to ensure that the originating party has CSDC service and that the carrier to be used provides 56 kb/s voice/data capability. A blocked call is routed to a special service error announcement. Non-CSDC calls are not allowed to route over CSDC-only carriers. Non-payer screening is not allowed for CSDC calls using CCIS signalling.

A CSDC call is routed directed to the carrier or indirectly via the Access Tandem (AT) or Signal Conversion Point (SCP). The call is terminated directly from the carrier to the end office or indirectly via the AT or SCP. Signalling for direct routing is either CCIS or EA-MF and is assigned on a trunk group basis.

The AT is an ESS switch which allows access to carriers from an end office without requiring direct trunks. Signalling between end offices and the AT is either EA-MF or CCIS. Trunks groups using EA-MF signalling can have combined carrier traffic. Separate trunk groups for each carrier are required for CCIS signalling.

The SCP is an ESS switch which allows access to carriers using only CCIS signalling from offices without the CCIS capability. Separate trunk groups for each carrier are used between the originating end office and the SCP. Separate trunk groups are optional between the SCP and the terminating end office and the terminating end office. Signalling between the end office and the SCP is MF. The SCP must have direct connection to the carrier using CCIS signalling.

=========================
=Remote Switching System=
=========================

The RSS can be used as a remote access point for CSDC. The compatibility of RSS and CSDC improves the marketability of both features. The RSS design allows a provision for the support of D4 special service channel bank plug-ins. This provision allows for such applications as off premises extensions, foreign exchanges lines, and private lines. Thus the RSS can be used as a CSDC access point in a configuration similar to the CSDC RX arrangement.

=Centrex/ESSX-1=

The CSDC feature is optionally available to Centrex/ESSX-1 customers. Most of the capabilities of Centrex service can be applied to Centrex lines that have been assigned the CSDC feature. In voice mode, the Centrex/CSDC line can exercise any of the Centrex group features that have been assigned to the line. In the voice/data mode, several Centrex features are inoperable or operate only on certain calls. The CSDC feature can be provided for a Centrex group as follows:

1. Message Network Basis (MTS)
2. IntraCentrex group basis
3. InterCentrex group basis
4. Any combination of the above

=User Perspective for the CSDC=

To establish a CSDC call, a CSDC user goes off hook, receives dial tone and dials. The dialing format for the CSDC/MTS is as follows for interim plan:

#99 AB (1+) 7 or 10 digits (#)

The customer dials '#99' to access the CSDC feature. The 'AB' digits are the carrier designation code. No dial tone is returned after the 'AB' digits. The 1+ prior to the 7 or 10 digit directory number must be used if it is required for MTS calls. The '#' at the end is optional, if it is not dialed, end of dialing is signalled by a time-out.

The long term dialing format for the CSDC/MTS is as follows:

#56 (10XXX) (1+) 7 or 10 digits (#)

Dialing '#56' indicates 56kb/s alternate voice/data transmission. the '10XXX' identifies the carrier to be used for the call. If '10XXX' is not dialed on an inter-LATA call, the primary carrier of the subscriber is used. If '10XXX' is not dialed on an intra-LATA call, the telco handles the call. The long term plan also allows for several abbreviated forms. Dialing '#56 10XXX #' is allowed for routing a call which prompts the customer to dial according to the carrier dialing plan. Dialing '#56 10XXX' followed by a speed call is also allowed. If a customer has pre-subscribed to a carrier which can carry CSDC calls and the CSDC access code is stored as part of the speed calling number, the customer dials the speed calling code to make a CSDC call.

Regular ringing is applied to the called line and audible ringing is applied to the calling terminal. Once the voice connection is established, either party can initiate the switch to data mode, if desired. To initiate a change in mode a CSDC user must initiate a mode switch command via a closure of the NCT

An example of a mode switch:

Suppose party A wants to switch to data. Party A issues a mode switch command and receives a signal called far end voice (FEV) which is a bipolar sequence (2031 hz at 60 ipm). Party A may now hang up the handset at any time after initiating the mode switch command. Party B receives a far end data (FED) tone (2031 Hz at 39 ipm) indicating party A wants to switch to data. If party B agrees to switch to data, party B must initiate a mode switch command. Party B may nor hang up the handset. Data transmission is now possible.

To switch to the voice mode, anyone can initiate it. To switch, party A would pick up the handset and initiate a mode switch command and will receive the FED tone. Party B receives the FEV tone indicating that party A wants to go voice. Party B must now pick up the hand set and initiate a mode switch command. To terminate a call, either party may just leave the handset on and indicate a mode switch. If termination is issued during a mode conflict, time out will disconnect the call, usually about 10 or 11 seconds.

Centrex/ESSX-1 customers may utilize the CSDC service in several ways if they have CSDC terminals with the necessary on premises equipment. The standard CSDC call is initiated by dialing the message network access code, (9). The dialing sequence is then identical to the plan for MTS:

#99 AB (1+) 7 or 10 digits (interim plan)

#56 (10XXX) (1+) 7 or 10 digits (#) (long term plan)

The dialing pattern to establish interCentrex or intraCentrex CSDC calls is as follows:

CSDC access code + extension

An intraCentrex/CSDC call is initiated by dialing the trunk access code assigned to route a loop-around Centrex/CSDC trunk group. Next, the extension of the desired station is dialed. To establish an interCentrex call a different trunk access code must be used to route the CSDC calls to another Centrex group instead of a station.

The CSDC maintenance circuit has a dialable digital loopback. This loopback is very useful in CSDC testing. A customer can check their access line by dialing the test DN. The loop is automatically activated when the call is answered.

```
================
=End of Part I.=
================
```

Part II: The CSDC hardware, and office data structures.

==Phrack Inc.==

Volume Two, Issue Ten, Phile #6 of 9

```
-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-
!                                   !
#       Hacking Primos Part I       #
!                                   !
#            By Evil Jay            #
!                                   !
#     Phone Phreakers of America    #
!                                   !
#            (C) 1986-87            #
!                                   !
-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-
```

Author Note:

I should begin by saying that there are other files out there about hacking Primos, one written recently, that basically tell you nothing at all as far as in-depth Primos is concerned. Those files should be deleted and this put in its place. This is the first in many files on Primos, and I will go into many topics, such as the on-line network, the different subsystems and other subjects. Hope you enjoy!

*** Gaining Entry Part 1 ***

Gaining entry, as always, is the hardest part.

When you call a Primos system it will connect with something like this:

```
PRIMENET 19.2.7F PPOA1
```

If it doesn't give a welcome msg like above trying typing something like "XXZZZUUU" and hit return and it should come back with:

```
Invalid command "XXZZZUUU".  (logo$cp)
Login please.
ER!
```

To login you type:

```
LOGIN <USER ID> <RETURN/ENTER>
```

Or Just:

```
LOGIN <RETURN/ENTER>
(Then it will ask for your "User ID?")
```

User ids differ from system to system but there are ALWAYS default accounts to try. For "User ID?" try...

```
SYSTEM (This is the operators account and with it you can usually do
        anything.)
LIB
DOS
```

After you enter your User ID it will prompt you with:

```
Password?
```

This is of course, where you enter your password. For SYSTEM try...

SYSTEM
SYSMAN
NETLINK
PRIMENET
MANAGER
OPERATOR

And anything else you can think of. These are just common passwords to these defaults.

For LIB try...

LIBRARY
SYSLIB
LIB
SYSTEM

For DOS try...

DOS
SYSDOS
SYSTEM

Etc...Just use your brain.

Older Versions

On older versions of Primos, 18 and below, you could enter one of the system defaults above and hit CTRL-C once or twice for the password and it would drop you into the system. Whether this is a bug or intentional I don't really have any idea. But it does work sometimes. To see what ver of Primos your trying to logon to just look at the welcome message when you logon:

```
PRIMENET 19.2.7F PPOA1
```

19 is the version number. So thus, if you were logging on to this particular Prime you would NOT be able to use the above mentioned bug/default-password.

By the way, if you do not know what version it is (because it did not give you a welcome msg when you connected...try to do the above mentioned anyway.)

Now, if it says:

```
Invalid user id or password; please try again.
```

Then you must try a different password. Notice, that the system informs you that either the User ID, the password or both are wrong. Don't worry about this...just hack the defaults. There have been a lot of rumors spreading around about common defaults such as: PHANTOM, PRIMOS, PRIME & FAM, but I believe this to be a load of shit. I have never seen a system with these defaults on them. But, as far as PRIMOS and PRIME go, these are sometimes common accounts but I really don't believe that they are defaults. Also try accounts like DEMO & GUEST. These are sometimes common accounts (but never very often).

Primos does not have limited commands before logon such as Tops 20 and DEC. So hacking a Primos is really nothing but taking a guess.

** No passwords **

Some users have been known to use a carriage return for their password which in other words means, once you enter your user id, your logged in without having to enter a password. Sometimes, these are default passwords assigned by the system operator, but that is rare. If you can get the format (perhaps you already have any account) for the regular user id's, then try passwords like:

NETLINK
SYSTEM
PRIME
PRIMENET
PRIMOS

And other typical user passwords like sex, hot, love...etc. Most female users that I have talked to on a local university prime all seem to have picked account that have something to do with sex...sex being the most popular.

** The Format **

The format for a user id can be just about ANYTHING the operators or system owners want...and they are usually random looking things that make no sense. They can be a combination of numbers, numbers and I am almost sure CTRL characters can be used. Lower & Upper case do not matter...the system, changes all lower case entry to upper case. Passwords can be anything up to 16 characters in length.

** Your In! **

If you get a valid ID/Password you will see something like this:

```
PPOA1 (user 39) logged in Monday, 15 Dec 86 02:29:16.
Welcome to PRIMOS version 19.4.9.
Last login Friday, 12 Dec 86 08:29:04.
```

Congratulate yourself, you just did something that should be called something of an achievement!

The next part will deal with very basic commands for beginners. I would like to end this part with a few more words. Yes, Primos is hard to hack, but given the time and patience almost every system has those basic demo accounts and CAN be hacked. Most hackers tend to stay away from Primes, little knowing that Primos is a system that is very entertaining and certainly kept me up late hours of the night. Have fun and keep on hacking. If you have any questions or comments, or I have made some sort of error, by all means get in touch with me at whatever system you have seen me on...

** Now For The Good Shit **

This part was originally going to be a beginners introduction to commands on a Primos system. Instead I decided to write a part which should help ANYONE with a low level account gain system access. I would also like to thank PHRACK Inc. on the wonderful job they are doing...without PHRACK I don't really know for sure how I would have distributed my files. Oh yes, I know of all the other newsletters and the like, but with PHRACK it was only a matter of getting a hold of one of the people in charge, which is a simple matter since their mailbox number is widely known to the hack/phreak community. I would also like to encourage boards of this nature to support PHRACK fully, and I would also like to congratulate you guys, once again, for the great job your doing. Now, on with the file.

** Stuff You Should Know **

The explanation I am going to (try to) explain will NOT work all the time... probably 60% of the time. Since I discovered this, or at least was the first to put it in "print" I would at least ask those system operators out there to keep my credits and the credits of my group in this file.

** Some More Stuff **

First, this is not exactly a "novice"-friendly file. You should be familiar with the ATTACH and SLIST commands before proceeding. They are quite easy to learn, and it is really not required to use this file, but just the same, these are important commands in learning the Primos system so you should at least be familiar with them. To get help on them type:

```
HELP SLIST
```

or

```
HELP ATTACH
```

You should also play with the commands until you know all of their uses.

** Okay, Here We Go **

This file is not going to explain everything I do. I'm just going to show you how to get SYS1 privileged accounts.

First, log on to your low access account.

Type:

```
ATTACH MFD
```

Then get a DIR using:

```
LD
```

Okay, your now seeing a dir with a lot of sub-directories. The only files that should be in the main directory (most of the time) are BOOT and SYS1. Ignore these...look for a file called CCUTIL or something with the word UTILITY or

UTIL or UTILITIES...something that looks like UTILITY...

Okay, ATTACH to that directory with:

```
ATTACH <NAME OF DIRECTORY>
```

Now, do an LD again and look at the files. Now, here is the part that is really random. Since not every PRIME system will have the same UTILITY programs, just look at any that have an extension ".CPL". There might be one called USRLST.CPL. Type:

```
SLIST USRLST <NO NEED TO TYPE ".CPL" AT THE END.>
```

Okay, it should be printing a whole bunch of bullshit. Now in this program there SHOULD be a line that looks like the following:

```
A CCUTIL X
```

Now, CCUTIL is the name of the dir you are on so I have to point out that CCUTIL WILL NOT ALWAYS BE THE NAME OF THAT UTILITY DIRECTORY. So if the name of the UTILITY directory you are on is called UTILITY then the line will look like this:

```
A UTILITY X
```

Now, the X is the PASSWORD OF THAT DIRECTORY. AGAIN, IT CAN BE ANYTHING. The password may be UTILITY which means it will look like this:

```
A UTILITY UTILITY
```

Or the password may be SECRET. So:

```
A UTILITY SECRET
```

Pat yourself on the ass...you know have SYS1 access. Log back in with the LOGIN command (or if it doesn't work just LOGOUT and LOGIN again). Enter UTILITY or CCUTIL (or WHATEVER THE NAME OF THE DIRECTORY WAS) as the user id. Then for the password just enter the password. If this doesn't work, then what you will have to do is try out other sub-directories from the MFD directory. Then SLIST other programs with the extension. In one of my other PRIME files I will fully explain what I have just done and other ways to get the directories/ids password.

Now, if you don't see any line in the program like:

```
S <NAME OF DIR> <PASSWORD>
```

Then list other programs in the utility program or try other directories. I have gained SYS1 access like this 60% of them time. And NOT ALWAYS ON THE UTILITY DIRECTORY.

That is about it for this file. Stay tuned for a future PHRACK issue with another PRIME file from me. If I don't change my mind again, the next file will deal with basic commands for beginners.

```
-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-
!                                   !
#         This Has Been An:         #
!                                   !
#       Evil Jay Presentation       #
!                                   !
#     Phone Phreaks of  America     #
!                                   !
#            (C) 1986-87            #
!                                   !
-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-#-
```

==Phrack Inc.==

Volume Two, Issue Ten, Phile #7 of 9

Automatic Number Idenfification

Written by Doom Prophet and Phantom Phreaker

Automatic Number Identification (ANI) is nothing more than automatic means for immediately identifying the Directory Number of a calling subscriber. This process made it possible to utilize CAMA* (Centralized Automatic Message Accounting) systems in SxS, Panel, and Xbar #1 offices.

The identity of the calling line is determined by ANI circuits installed in the types of CO's mentioned above. Xbar#5 offices have their own AMA (Automatic Message Accounting) equipment and utilize an AMA translator for automatically identifying the calling line.

Before ANI was developed, each subscriber line (also called a local loop) had a mechanical marking device that kept track of toll charges. These devices were manually photographed at the end of the billing period and the amount of the subscribers bill was determined from that. This process was time consuming, so a new system (ANI) was developed.

The major components of the ANI system used in SxS and Crossbar #1 are:

Directory number network and bus arrangement* for connecting the sleeve(the lead that is added to the R(ing) and T(ip) wires of a cable pair at the MDF* (Main Distribution Frame));

A lead of each line number through an identifier connector to the identifier circuit;

Outpulser and Identifier connector circuit to seize an idle Identifier;

Identifier circuit to ascertain the calling party's number and send it to the outpulser for subsequent transmission through the outpulser link to the ANI outgoing trunk;

An ANI outgoing trunk to a Tandem office equipped with a CAMA system.

The following is a synopsis of the ANI operations with respect to a toll call through a #1Xbar office. The call is handled in the normal manner by the CO equipment and is routed through an ANI outgoing trunk to a Tandem office. The identification process starts as soon as all digits of the called number are received by the CAMA sender in the Tandem office and when the district junctor in the Xbar office advances to its cut-through position (a position of the connecting circuits or paths between the line-link and trunk-link frames in the CO).

Upon receiving the start identification signal from the CAMA equipment, the ANI outgoing trunk (OGT) establishes a connection through an outpulser link to an idle outpulser circuit. An idle identifier is then seized by the outpulser circuit through an internal Identifier connector unit. Then the identifier through the connector unit connects to the directory number network and bus system.

At the same time, the identifier will signal the ANI trunk to apply a 5800Hz identification tone to the sleeve lead of the ANI trunk. The tone is transmitted at a two-volt level over the S lead paths through the directory number network and bus system. It will be attenuated or decreased to the microvolt range by the time the identifier circuit is reached, necessitating a 120dB voltage amplification by the amplifier detector equipment in the identifier to insure proper digit identification and registration operations.

A single ANI installation can serve as many as six CO's in a multi-office building. The identifier starts its search for the calling line number by testing or scanning successively the thousands secondary buses of each CO. When the 5800Hz signal is detected, the identifier grounds corresponding leads to the outpulser, to first register the digit of the calling office and then the thousands digit of the calling subscriber's number. The outpulser immediately translates the digit representing the calling office code into its own corresponding three digit office code. The identifier continues its scanning process successively on the groups of hundreds, tens, and units secondary buses in the calling office, and the identified digits of the calling number are also registered and translated in the outpulser's relay equipment for transmission to the tandem office.
The outpulser is equipped with checking and timing features to promptly detect and record troubles encountered (This process may be responsible for some of the cards found while trashing). Upon completion of the scanning process, it releases the identifier and proceeds to outpulse in MF tones the complete calling subscriber's number to the CAMA equipment in the tandem office in the format of KP+X+PRE+SUFF+ST where the X is an information digit. The information digits are as follows:

0-Automatic Identification (normal)   1-Operator Identification (ONI)*
2-Identification Failure (ANIF)*

(There is also other types of outpulsing of ANI information if the calling line has some sort of restriction on it).

When all digits have been transmitted and the ANI trunk is cut-through for talking, the outpulser releases.

In the tandem office, the calling party's number is recorded on tape in the CAMA equipment together with other data required for billing purposes. This information, including the time of when the called station answered and the time of disconnect, goes on AMA tapes.
The tapes themselves are usually standard reel to reel magnetic tape, and are sent to the Revenue Accounting Office or RAO at the end of the billing period.

So, to sum the entire ANI process up:

The toll call is made. The CO routes the call through ANI trunks where an idle identifier is seized which then connects to the directory number network and bus system while signalling the ANI trunk to apply the needed 5800Hz tone to the Sleeve. The identifier begins a scanning process and determines the calling office number and the digits of the calling subscriber's number, which is sent by way of the outpulser in MF tones to the CAMA equipment in the tandem office. The call information is recorded onto AMA tapes and used to determine billing.

Note that your number does show up on the AMA tape, if the circumstances are correct, (any toll call, whether it is from a message-rate line or from a flat-rate line). However, the AMA tapes do not record the calling line number in any separated format. They are recorded on a first-come, first-serve basis.

Misc. Footnotes (denoted by an asterisk in the main article)
----

* ANIF-Automatic Number Identification Failure. This is when the ANI equipment does not work properly, and could occur due to a wide variety of technicalities. When ANIF occurs, something called ONI (Operator Number Identification) is used. The call is forwarded to a TSPS operator who requests the calling line number by saying something similar to 'What number are you calling from?'

* CAMA-Centralized Automatic Message Accounting. CAMA is a system that records call details for billing purposes. CAMA is used from a centralized location, usually a Tandem office. CAMA is usually used to serve class 5 End Offices in a rural area near a large city which contains a Tandem or Toll Office. CAMA is similar to LAMA, except LAMA is localized in a specific CO and CAMA is not.

* The Directory Number Network and bus system is a network involved with the ANI process. It is a grid of vertical and horizontal buses, grouped and classified as Primary or Secondary. There are 100 vertical and 100 horizontal buses in the Primary system. In the Secondary system, there are two sub-groups:Bus system #1 and Bus system #2, both of which have ten horizontal and vertical buses. These buses as a whole are linked to the Identifier in the ANI trunk and are responsible for identifying tens, hundreds, thousands and units digits of the calling number (After the Identifier begins its scanning process).

* MDF-Main Distribution Frame. This is the area where all cable pairs of a certain office meet, and a third wire, the Sleeve wire, is added. The Sleeve wire is what is used in gathering ANI information, as well as determining a called lines status (off/on hook) in certain switching systems by presence of voltage. (voltage present on Sleeve, line is busy, no voltage, line is idle.)

* ONI-Operator Number Identification. See ANIF footnote.

NOTE: There are also other forms of Automatic Message Accounting, such as LAMA (Local Automatic Message Accounting). LAMA is used in the class 5 End Office as opposed to CAMA in a Toll Office. If your End Office had LAMA, then the ANI information would be recorded at the local level and sent from there. The LAMA arrangement may be computerized, in which it would denoted with a C included (LAMA-C or C-LAMA).

References and acknowledgements

Basic Telephone Switching Systems (Second Edition) by David Talley
Understanding Telephone Electronics by Radio Shack/Texas Instruments

Other sysops are allowed to use this file on their systems as long as none of it is altered in any way.

-End of file-
Jul 12 1986

==Phrack Inc.==

Volume Two, Issue Ten, Phile #8 of 9

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

In PWN Issue Seven/Part One, we had an article entitled "Maxfield Strikes Again." It was about a system known as "THE BOARD" in the Detroit 313 NPA. The number was 313-592-4143 and the newuser password was "HEL-N555,ELITE,3" (then return). It was kind of unique because it was run off of an HP2000 computer. On August 20, 1986 the following message was seen on "THE BOARD."

```
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
-
                Welcome to MIKE WENDLAND'S I-TEAM sting board!
                   (Computer Services Provided By BOARDSCAN)
                             66 Megabytes Strong

                           300/1200 baud - 24 hours.

                        Three (3) lines = no busy signals!
                          Rotary hunting on 313-534-0400.


Board:   General Information & BBS's
Message: 41
Title:   YOU'VE BEEN HAD!!!
To:      ALL
From:    HIGH TECH
Posted:   8/20/86 @ 12.08 hours
```

Greetings:

You are now on THE BOARD, a "sting" BBS operated by MIKE WENDLAND of the WDIV-TV I-Team. The purpose? To demonstrate and document the extent of criminal and potentially illegal hacking and telephone fraud activity by the so-called "hacking community."

Thanks for your cooperation. In the past month and a half, we've received all sorts of information from you implicating many of you to credit card fraud, telephone billing fraud, vandalism, and possible break-ins to government or public safety computers. And the beauty of this is we have your posts, your E-Mail and--- most importantly ---your REAL names and addresses.

What are we going to do with it? Stay tuned to News 4. I plan a special series of reports about our experiences with THE BOARD, which saw users check in from coast-to-coast and Canada, users ranging in age from 12 to 48. For our regular users, I have been known as High Tech, among other ID's. John Maxfield of Boardscan served as our consultant and provided the HP2000 that this "sting" ran on. Through call forwarding and other conveniences made possible by telephone technology, the BBS operated remotely here in the Detroit area.

When will our reports be ready? In a few weeks. We now will be contacting many of you directly, talking with law enforcement and security agents from credit card companies and the telephone services.

It should be a hell of a series. Thanks for your help. And don't bother trying any harassment. Remember, we've got YOUR real names.

Mike Wendland
The I-team
WDIV, Detroit, MI.

- -

This then is the result:

Phrack World News proudly presents...

Mike Wendland & the I-Team Investigate
"Electronic Gangsters"

- -

Carman Harlan: Well we've all heard of computer hackers, those electronic gangsters who try to break into other people's computer systems. Tonight on the first of a three part news 4 [WDIV-TV, Channel 4 in Detroit] extra, Mike Wendland and the I-Team will investigate how such computer antics jeopardize our privacy. Mike joins us now to tell us what at first may have been innocent fun may now be affecting our pocket books.

Mike Wendland: Well Carman and Mort, thanks to the media and movies just about everyone knows about hackers and phone phreaks. By hooking their Apples, their Ataris, and their Commodores into telephone lines these electronic enthusiasts have developed a new form of communication, the computer bulletin board. There are probably 10,000 of these message swapping boards around the country today, most are innocent and worthwhile. There are an estimated 1,000 pirate or hacker boards where the main activities are electronic trespassing, and crime [Estimates provided by John Maxfield].

[Clipping From Wargames comes on]

In movies like Wargames computer hackers are portrayed as innocent hobbyist explorers acting more out of mischief than malice. But today a new generation of hackers have emerged. A hacker that uses his knowledge of computers to commit crimes. Hackers have electronically broken into banks, ripped off telephone companies for millions of dollars, trafficked in stolen credit card numbers, and through there network of computer bulletin boards traded information on everything from making bombs to causing terrorism.

[Picture of John Maxfield comes on]

John Maxfield: Well, now there are electronic gangsters, not just electronic explorers they are actually gangsters. These hackers meet electronically through the phone lines or computer bulletin boards. They don't meet face to face usually, but it is a semi-organized gang stile activity, much like a street gang, or motorcycle gang.

Mike Wendland: John Maxfield of Detroit is America's foremost "Hacker Tracker". He has worked for the F.B.I. and various other law enforcement and security organizations. Helping catch dozens of hackers around the country, who have used their computers for illegal purposes. To find out how widespread these electronic gangsters have become, we used John Maxfield as a consultant to setup a so-called "sting" bulletin board [THE BOARD].

We wrote and designed a special program that would allow us to monitor the calls we received and to carefully monitor the information that was being posted. We called our undercover operation "The Board", and put the word out on the underground hacker network that a new bulletin board was in operation for the "Elite Hacker". Then we sat back and watched the computer calls roll in.

In all we ran our so called "Sting" board for about a month and a half, 24 hours a day, 7 days a week. We received literally hundreds of phone calls from hackers coast to coast, ranging in age from 17 to 43. All of them though had one thing in common, they were looking for ways to cheat the system.

The hackers identified themselves by nicknames or handles like CB radio operators use, calling themselves things like Ax Murderer, Big Foot, and Captain Magic. They left messages on a variety of questionable subjects, this hacker for instance told how to confidentially eavesdrop on drug enforcement radio conversations. A New York hacker called The Jolter swapped information on making free long-distance calls through stolen access codes, and plenty of others offered credit card numbers to make illegal purchases on someone else's account.

John Maxfield: Well these kids trade these credit card numbers through the computer bulletin boards much like they'd trade baseball cards at school. What we've seen in the last few years is a series of hacker gangs that are run by an adult, sort of the mastermind who stays in the background and is the one who fences the merchandise that the kids order with the stolen credit cards.

Mike Wendland: Then there were the malicious messages that had the potential to do great harm. The Repo Man from West Virginia left this message telling hackers precisely how to break into a hospital computer in the Charleston, WV area.

[Picture of Hospital]

This is where that number rings, the Charleston Area Medical Center. We immediately notified the hospital that there computer security had been breached. Through a spokesperson, the hospital said that a hacker had indeed broken into the hospital's computer and had altered billing records. They immediately tightened security and began an investigation. They caught the hacker who has agreed to make restitution for the damages. Maxfield says though, "Most such break-ins are never solved".

John Maxfield: When you are talking about electronic computer intrusion, it's the perfect crime. It's all done anonymously, it's all done by wires, there's no foot prints, no finger prints, no blood stains, no smoking guns, nothing. You may not even know the system has been penetrated.

Mike Wendland: Our experience with the "Sting" bulletin board came to a sudden and unexpected end. Our cover was blown when the hackers somehow obtained confidential telephone company records. The result a campaign of harassment and threats that raised serious questions about just how private our supposedly personal records really are. That part of the story tomorrow. [For a little more detail about how their cover was "blown" see PWN Issue 7/Part One, "Maxfield Strikes Again." Heh heh heh heh.]

Mort Crim: So these aren't just kids on a lark anymore, but who are the hackers?

Mike Wendland: I'd say most of them are teenagers, our investigation has linked about 50 of them hardcore around this area, but most very young.

Mort Crim: Far beyond just vandalism!

Mike Wendland: Yep.

- -

A few quicknotes in between shows, Mike Wendland and John Maxfield set up THE BOARD. Carman Harlan and Mort Crim are newscasters.

Also if anyone is interested in the stupidity of Mike Wendland, he flashed the post that contained the phone number to the hospital across the screen, Bad Subscript put the VCR on pause and got the number. If interested please contact Bad Subscript, Ctrl C, or myself.

- -

Carman Harlan: Tonight on the second part of a news 4 [WDIV-TV, Channel 4 in Detroit] extra Mike Wendland and the I-Team report on how they setup a sting bulletin board to see how much they could get on these criminal hackers. Mike joins us now to explain that information, that was not the only thing they got.

Mike Wendland: That's right, Carman & Mort. Our so called sting bulletin board received hundreds of calls from hackers all over America, and even Canada. They offered to trade stolen credit cards, and they told how to electronically break into sensitive government computers. But our investigation came to a sudden end when our sting board was stung. Our cover was blown when a hacker discovered that this man, computer security expert John Maxfield was serving as the I-Team consultant on the investigation. Maxfield specializes as a hacker tracker and has worked for the F.B.I. and various other police and security agencies. The hacker discovered our sting board by getting a hold of Maxfield's supposedly confidential telephone records.

John Maxfield: And in the process of doing that he discovered the real number to the computer. We were using a different phone number that was call forwarded to the true phone number, he found that number out and called it to discover he was on the sting board.

Mike Wendland: But the hacker didn't stop at exposing the sting, instead he posted copies of Maxfield's private telephone bill on other hacker bulletin boards across the country.

John Maxfield: The harassment started, all of the people on my phone bill got calls from hackers. In some cases their phone records were also stolen, friends and relatives of theirs got calls from hackers. There was all sorts of other harassment, I got a call from a food service in Los Angeles asking where I wanted the 500 pounds of pumpkins delivered. Some of these kids are running around with guns, several of them made threats that they were going to come to Detroit, shoot me and shoot Mike Wendland.

Mike Wendland: A spokesperson from Michigan Bell said that the breakdown in security that led to the release of Maxfield's confidential records was unprecedented.

Phil Jones (MI Bell): I think as a company were very concerned because we work very hard to protect the confidentially of customer's records. [Yeah, right].

Mike Wendland: The hacker who got a hold of Maxfield's confidential phone records is far removed from Michigan, he lives in Brooklyn, NY and goes by the name Little David [Bill From RNOC]. He says that getting confidential records from Michigan Bell or any other phone company is child's play. Little David is 17 years old. He refused to appear on camera, but did admit that he conned the phone company out of releasing the records by simply posing as Maxfield. He said that he has also sold pirated long-distance access codes, and confidential information obtained by hacking into the consumer credit files of T.R.W. Little David says that one of his customers is a skip-tracer, a private investigator from California who specializes in finding missing people. Maxfield, meanwhile, says that his own information verified Little David's claim.

John Maxfield: The nearest I can determine the skip-tracer was using the hacker, the 17 year old boy to find out the whereabouts of people he was paid to find. He did this by getting into the credit bureau records for the private eye. This is an invasion of privacy, but it's my understanding that this boy was getting paid for his services.

Mike Wendland: In Long Island in New York, Maxfield's telephone records were also posted on a bulletin board sponsored by Eric Corley, publisher of a hacker newsletter [2600 Magazine]. Corley doesn't dispute the harassment that Maxfield received.

Eric Corley: Any group can harass any other group, the difference with hackers is that they know how to use particular technology to do it. If you get a malevolent hacker mad at you there's no telling all the different things that can happen.

Mike Wendland: What can happen? Well besides getting your credit card number or charging things to your account, hackers have been known to change people's credit ratings. It is really serious business! And tomorrow night we'll hear about the hacker philosophy which holds that if there is information out there about you it is fair game.

Mort Crim: "1984" in 1986.

Mike Wendland: It is!

- -

Carman Harlan: News four [WDIV-TV, Channel 4 in Detroit] extra, Mike Wendland and the I-Team look at how these hackers are getting out of hand.

Mike Wendland: The problem with hackers is not just with mischief anymore, unscrupulous hackers are not only invading your privacy, they are costing you money. Case and point, your telephone bills, because American telephone companies have long been targets of computer hackers and thieves we are paying more than we should.

Experts say the long distance companies lose tens of millions of dollars a year to, these self described "Phone Phreaks."

For example in Lansing, the Michigan Association of Governmental Employees received a phone bill totalling nearly three hundred and twenty one thousand dollars. For calls illegally racked up on there credit card by hackers. Such victims seldom get stuck paying the charges, so hackers claim there piracy is innocent fun.

Phil Jones (MI Bell): Nothing could be further from the truth, it becomes a very costly kind of fun. What happens is that the majority of the customers who do pay there bills on time, and do use our service lawfully end up quitting after that bill.

Mike Wendland: That's not all, hackers regularly invade our privacy, they leave pirated credit card numbers and information how to break into electronic computer banks on bulletin boards. Thousands of such electronic message centers exist across the country, most operated by teenagers.

John Maxfield: There is no law enforcement, no parental guidance, they're just on their own so they can do anything they want. So the few bad ones that know how to steal and commit computer crimes teach the other ones.

Mike Wendland: There is very little that is safe from hackers, from automatic teller machines and banks to the internal telephone systems at the White House. Hackers have found ways around them all hackers even have their own underground publication of sorts that tells them how to do it.

[Close up of publication]

Its called 2600 [2600 Magazine], after the 2600 hertz that phone phreaks use to bypass telephone companies billing equipment. It tells you how to find credit card numbers and confidential records in trash bins, break into private mainframe computers, access airline's computers, and find financial information on other people through the nations largest credit bureau, TRW. 2600 is published in a ram-shackled old house at the far end of Long Island, New York by this man, Eric Corley. He argues that hackers aren't electronic gangsters.

Eric Corley: We like to call them freedom fighters. Hackers are the true individuals of the computer revolution, they go were people tell them not to go, they find out things they weren't supposed to find out.

Mike Wendland: Corley's newsletter supports a hacker bulletin board called the Private Sector. Last year the F.B.I. raided it.

Eric Corley: They managed to charge the system operator with illegal possession of a burglary tool in the form of a computer program.

Mike Wendland: But the bulletin board is still in operation. Corley resents the suspicion that hackers are involved in criminal activities.

Eric Corley: Hackers are not the people who go around looking for credit cards and stealing merchandise. That's common thievery. Hackers are the people who explore. So basically what we are saying is more knowledge for more people. That will make it better for everybody.

Mike Wendland: He claims that hackers, in their own ways, really protect our rights by exposing our vulnerabilities. Well hackers may expose our vulnerabilities, but they also invade our privacy. There activities have really spotlighted the whole question of privacy raised by the massive files that are now out there in electronic data banks. Much of that information that we think is personal and confidential is often available to the whole world.

Original transcript gathered and typed by

Ctrl C & Bad Subscript

Major editing by Knight Lightning

_

==Phrack Inc.==

Volume Two, Issue Ten, Phile #9 of 9

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

On The Home Front   December 25, 1986

Happy Holidays to all from everyone at Phrack Inc. and Metal Shop Private!

Well, here we are at that time of year again and before too long we will have a new wave of self appointed hackers who got their modems for Christmas.

Some important dates to point out:

November 17, 1986............1st Anniversary of Phrack Inc.
January 2, 1987..............1st Anniversary of Metal Shop being a PRIVATE BBS.
January 10, 1987.............1st Anniversary of Metal Shop AE, now Quick Shop
January 25, 1987.............1st Anniversary of Phrack World News

The Phrack Inc./Metal Shop Private Voice Mailbox is now back in operation. If you have a question for Taran King, Cheap Shades, or myself and cannot reach us through regular means, please leave us a message on our VMS.

Thanks to the efforts of Oryan Quest, an upcoming Phrack Pro-Phile will focus on Steve Wozniak.

Plans are already underway for Summer Con '87. It is to be held in St. Louis, Missouri during the last week of June. It is being sponsored by TeleComputist Newsletter, Phrack Inc., and Metal Shop Private. Forest Ranger is in charge of planning and is putting out a lot of front money for the necessary conference rooms and such. There will be a mandatory $10 admittance at the door to Summer Con '87. If you will be attending this conference, please as an act of good faith and to save 50% send $5 in early to:

J. Thomas
TeleComputist Newsletter
P.O. Box 2003
Florissant, Missouri 63032-2003

Also, Letters to the Editor and anything else dealing with TeleComputist can be sent to the same address. TeleComputist can also be reached through Easylink at 62195770, MCI Telex at 650-240-6356, CIS at 72767,3207 and PLINK at OLS 631.
Try MCI and Easylink first.

Not much else to say... so keep learning and try not to get into any trouble.

:Knight Lightning

_

Computer Hackers Beware! - Senate Passes Computer Fraud And Abuse Act

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

On October 2, 1986, the US Senate unanimously passed the Computer Fraud and Abuse Act of 1986. The bill, S. 2281, imposes fines of up to $500,000 and/or prison terms of up to 20 years for breaking into government or financial institutions' computers.

The Federal Government alone operates more than 18,000 medium-scale and large-scale computers at some 4,500 different sites. The Office of Technology Assessment estimates the government's investment in computers over the past four years at roughly $60 million. The General Services Administration estimates that there will be 250,000 to 500,000 computers in use by the Federal Government by 1990.

In 1984, legislators' attention to and concern about computer fraud was heightened by a report by the American Bar Association task force on computer crime. According to the report, based on a survey of 1,000 private organizations and public agencies, forty-five percent of the 283 respondents had been victimized by some form of computer crime, and more than 25 percent had sustained financial losses totaling between an estimated $145 million and $730 million during one twelve month period.

To address this problem, the Senate and House enacted, in 1984, the first computer statute (18 U.S.C. 1030). Early this year both the House and Senate introduced legislation to expand and amend this statute.

In the current bill, which is expected to be signed by President Reagan next week, penalties will be imposed on anyone who knowingly or intentionally accesses a computer without authorization, or exceeds authorized access and:

(1) Obtains from government computers information relating to national defense and foreign relations.

(2) Obtains information contained in financial records of financial institutions.

(3) Affects the use of the government's operation of a computer in any department or agency of the government that is exclusively for the use of the U.S. Government.

(4) Obtains anything of value, unless the object of the fraud and the thing

obtained consists only of the use of the computer.

(5) Alters, damages, or destroys information in any federal interest computer, or prevents authorized use of any such computer or information.

Under the bill, a person would be guilty of computer fraud if he or she causes a loss of $1,000 or more during any one year period.

Depending on the offense, penalties include fines up to $100,000 for a misdemeanor, $250,000 for a felony, $500,000 if the crime is committed by an organization, and prison terms of up to 20 years.

The bill also prohibits traffic in passwords and other information from computers used for interstate or foreign commerce. This part of the bill makes it possible for Federal Prosecutors to crack down on pirate bulletin boards and similar operations because the bill covers business computers, online networks, and online news and information services, all of which are considered interstate commerce.

Information provided by

P-80 Systems

GTE News December 20, 1986

"GTE Develops High-Speed GaAs Multiplexer Combining Four Data Channels"

In an effort to achieve data communication rates of several gigabits per second, GTE Labs (Waltham, MA) is combining the high-capacity of fiber optics with the high speed of gallium arsenide circuits. The research arm of GTE has designed a GaAs multiplexer that can combine four data channels, each with a communication rate of 1 gigabit per second, into one channel. GTE has also recently developed a technique called MOVPE (metal-organic vapor-phase epitaxy) for efficiently growing thin-film GaAs crystals.

The new devices should play an important role in future communication systems, which will involve high-capacity fiber-optic cables connecting houses and offices through telephone switching centres. Data rates on these cables could be as high as 20 gigabits per second. In addition to standard computer data, numerous video channels could be supported, each with a data rate of almost 100 megabits per second. The GaAs multiplexers will probably be the only devices fast enough to interface houses and offices through this fiber-optic grid. In future supercomputers [misuse of the word -eds.] these multiplexers will also be used for high-speed fiber-optic transmissions between various boards in the computer, replacing copper wires. Because of the high-speed nature of the fiber-optic link, such techniques may even be used for chip-to-chip communication.

GTE said it has completed a prototype of the GaAs multiplexer and a final version should be ready in less than a year.

Comments: And meanwhile, while GTE's been building gigabit/second multiplexers, AT&T Bell Labs is still experimenting with the neuron webs from slug brains...

Information from Byte Magazine, December 1986, Page 9

Typed & Commented on by Mark Tabas

_

The LOD/H Technical Journal

The Legion Of Doom/Hackers Technical Journal is a soft-copy free newsletter whose primary purpose is to further the knowledge of those who are interested in topics such as: Telecommunications, Datacommunications, Computer & Physical
Security/Insecurity and the various technical aspects of the phone system.

The articles are totally original unless otherwise stated. All sources of information for a specific article are listed in the introduction or conclusion
of the article. They will not accept any articles that are unoriginal, plagiarized, or contain invalid or false information. Articles will be accepted from anyone who meets those criteria. They are not dependant upon readers for articles, since members of LOD/H and a select group of others will be the primary contributors, but anyone can submit articles.

There is no set date for releasing issues, as they have no monetary or legal obligation to the readers, but they predict that issues will be released every 2 or 3 months. Thus, expect 4 to 6 issues a year assuming that they continue to produce them, which they intend to do.

The bulletin boards sponsoring the LOD/H TJs include:

Atlantis
Digital Logic Data Service
Hell Phrozen Over (HPO)
Metal Shop Private
Private Sector
The Shack //

- -
-

The first issue will include these articles;

- Introduction to the LOD/H Technical Journal and Table Of Contents

- Editorial: "Is the law a deterrent to computer crime?" by Lex Luthor

- Local Area Signalling Services (LASS) by The Videosmith

- Identifying and Defeating Physical Security and Intrusion Detection Systems Part I: The Perimeter by Lex Luthor

- Traffic Service Position System (TSPS) by The Marauder

- Hacking DEC's TOPS-20: Intro by Blue Archer

- Building your own Blue Box (Includes Schematic) by Jester Sluggo

- Intelligence and Interrogation Processes by Master Of Impact

- The Outside Loop Distribution Plant: Part I by Phucked Agent 04

- The Outside Loop Distribution Plant: Part II by Phucked Agent 04

- LOH Telenet Directory: Update #4 (12-9-86) Part I by LOH

- LOH Telenet Directory: Update #4 (12-9-86) Part II by LOH

- Network News & Notes by "Staff"

That's a total of 13 files...

That ends the preview, the newsletter is due to be released by January 1, 1987 so watch for it!

Information Provided by

Lex Luthor & The Legion Of Doom/Hackers Technical Journal Staff

Texas Rumors Run Rampant December 24, 1986

Remember all that controversy about Sir Gamelord being Videosmith?

Well here's the story...

It all started on a conference bridge, where a number of people including Evil Jay, Line Breaker [who, indirectly started all of this], and Blade Runner among others were having a discussion.

Line Breaker was telling a story of how Videosmith was a fed, how Videosmith had busted everyone at a phreak con (or something like that), and how he [Line Breaker] and some other people called Videosmith up, pretending to be feds, and got him to admit that he did these things.

Blade Runner was terribly pissed at Sir Gamelord (who had recently attempted to take over P.H.I.R.M., which is Blade Runner's group). As a retaliatory strike and after hearing this slander upon Videosmith's name, Blade Runner started telling people that Sir Gamelord was Videosmith. The stories have been getting more and more exaggerated since then but that is all that really happened.

[They say everything is bigger in Texas...I guess that includes bullshit too!]

Information Provided by Evil Jay

The Cracker Disappears December 27, 1986

The rumors and stories are flying around about the disappearance of one Bill Landreth aka The Cracker.

Bill Landreth is the author of "Out Of The Inner Circle," a book on hackers that was published a few years back.

According to newspaper articles in the San Francisco area, Bill was at a friend's home working on some computer program. His friend stepped out for a while and when he returned, there was a lot of garbage on screen and a suicide message.

On Ripco BBS, message was posted about Bill Landreth, stating that he had disappeared, and was once again wanted by the FBI. The message asked that anyone in contact with Bill would tell him to contact his "friends."

Most of what is going on right now is bogus rumors. There may be a follow up story in the next PWN.

Information Provided By

The Prophet/Sir Frances Drake/Elric Of Imrryr

_

U.S. Sprint Screws Up   December 24, 1986

Taken From the Fort Lauderdale Sun Sentinal

"He got a 1,400 page bill!"

In Montrose, Colorado, Brad Switzer said he thought the box from the U.S. Sprint Long Distance Company was an early Christmas present until he opened it
and found that it contained a 1,400 page phone bill.

The $34,000 bill was delivered to Switzer's doorstep Monday. He called U.S. Sprint's Denver office, where company officials assured him he was "Off the Hook." A spokesman for U.S. Sprint said that Switzer had mistakenly received U.S. Sprint's own phone bill for long distance calls.

Typed For PWN by The Leftist

_