==Phrack Inc.==

Volume Two, Issue 24, File 1 of 13

Phrack Inc. Newsletter Issue XXIV Index

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

February 25, 1989

Welcome to Phrack Inc. Issue 24. We're happy to be able to say that we've
been keeping with our proposed release dates recently as opposed to our problems with delays in the past.

A little clearing up needs to be done briefly. We have received questions
about the volume number being only 2 when, year-wise, it should be at about 4. In our opinion, a volume consists of 12 issues, ideally having 1 issue per month. Unfortunately, we have not been able, in the past, to keep up the pace.
If you're looking forward to a volume change, though, watch for issue 25 to lead into Volume 3 of Phrack Inc.

A brief announcement about SummerCon '89 appears in Phrack World News XXIV
and more details will be released as they develop.

As always, we ask that anyone with network access drop us a line to either
our Bitnet accounts or our Internet addresses (see signoff).

In this issue, we feature the conclusion of the Future Transcendent Saga as well as a supplement file of sorts to it called Advanced Bitnet Procedures submitted by VAXBusters International. We hope you enjoy it!

Taran King
C488869@UMCVMB.BITNET
C488869@UMCVMB.MISSOURI.EDU

Knight Lightning
C483307@UMCVMB.BITNET
C483307@UMCVMB.MISSOURI.EDU

Table of Contents:

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

==Phrack Inc.==

Volume Two, Issue 24, File 2 of 13

==Phrack Pro-Phile XXIV==

Created and Written by Taran King

Done on February 3, 1989

Welcome to Phrack Pro-Phile XXII. Phrack Pro-Phile was created to bring information to you, the community, about retired or highly important/ controversial people. This issue, I present one of the more rare sights in the world of phreaking and hacking...a female! She was vaguely active and had a few contacts with people that were largely involved with the community...

Chanda Leir
~~~~~~~~~~~

Handle:	Chanda Leir
Call Her:	Karen
Past Handles:	None
Handle Origin:	An aunt of hers as a child wanted to use this name is she ever became famous.
Date Of Birth:	May 8, 1970
Current Age:	Almost 19
Height:	5' 6"
Weight:	125 lbs. (providing Freshman 15 hasn't yet hit)
Eye Color:	Green/Grey
Hair Color:	Blond
Computers:	Her father is a real estate broker, so she began on a TI 700 terminal (an MLS Terminal)... just a modem and a keyboard and a scroll of PAPER)... then it was dad's business computer-- the KAYPRO II... Now she uses the Macs and the Sun systems and the IBM RT's located at CMU.

Karen started using BBSes in the D.C. area in 1983 (at the ripe age of 13). A guy by the name of Hack-Man (she supposes this was the "original" H-M) was running a board off of the dead side of the local 678 loop. Her introduction to phone "stuff" began when she called the "board" one day and found instead 30 people on the line instead of a carrier.

She was dumbfounded, and being female, there were 30 guys on the conference ready and willing to provide her with information as to origins of loops, conferences, boxing, etc. Scott (Hack-Man) later filled her in on the rest, gave her more numbers and such and that's where it all began.

The memorable phreakers or hackers that Karen has met include Cheshire Cat, Tuc, Bioc Agent 003 and anyone else who was at the TAP meeting during Thanksgiving of 1984.

She gained her experience by asking a LOT of questions to a lot of hard-up guys who were willing to give her all kinds of info since she was a girl. She attributes her information mostly to just taking in and remembering all of the information that people gave her.
~~~~~~~~~~~

The two boards that Karen listed as memorable were both in Falls Church, VA. which were Mobius Strip and Xevious II.

Currently she's a freshman at Carnegie Mellon University in Pittsburgh (or as she likes to call it, COMPUTER U.). Her major is probably "Policy & Management."

Her major accomplishment is that she was probably the youngest girl ever to attend a TAP meeting (at the age of 14) and probably one of the only people to attend one with Mom, Dad, and Aunt Linda (how embarrassing).

One of the reasons she quit the phreak/hack world was because of a visit from the Secret Service in February 1985... although they didn't really come for her... A "friend" wanted for credit card fraud called her while his line was hooked to a pin register.

The same weekend he called Karen, was Inauguration Weekend and she and her brother called the 456 (White House) loop something like 21 times in the 4-day weekend period... In any case the SS wanted to catch Eric and when her number showed up in two places, they decided to investigate. Freaked out her parents!

The real reason she quit the phreak/hack world was because she transferred high
schools in 1985 and became one of the "popular" kids and gained a social life, thus losing time and interest for the computer.

Chanda Lier's Interests Include: MUSIC... specifically harDCore... (that would be punk rock from Washington, DC). Most of her friends are or were in DC bands... The Untouchables, Teen Idles, Minor Threat, Youth Brigade (DC), Grey Matter, Government Issue, etc.

HORROR... novels, movies, comics.... Clive Barker, Arcane Comix (of which her friend Steve is publisher of), Peter Straub, Dean Koontz, Whitely Streiber etc... that whole genre...
And Flannery O'Connor rules...

Her most memorable experiences include the following:

Her parents used to "make" her start conferences for them whenever it was a relative's birthday. They would get the whole family on the line and chat and stuff. Everyone thought it was really cool....

Other fun times were when her dad would pull out his DoD (Department of Defense) phonebook and they would hack around for modem lines....

Tuc coming to her grandmother's house in April 1985 and then going to see "Desperately Seeking Susan"...

Some People to Mention:

"I guess, just Taran King, for this interview, and Knight Lightning...both
of whom contacted me here at CMU.... and TUC... and ...?"

-

And of course...that regular closing to the Phrack Pro-Phile... Are most of the phreaks and hackers that you've met computer geeks? "YES... no doubt."

Thanks for your time, Karen.

Taran King

==Phrack Inc.==

Volume Two, Issue 24, File 3 of 13

```
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
<>                                                            <>
<>                     Limbo To Infinity                      <>
<>                     ~~~~~~~~~~~~~~~~~                      <>
<>        Chapter Three of The Future Transcendent Saga       <>
<>                                                            <>
<>      Traversing The Barriers For Gateway Communication     <>
<>                                                            <>
<>               Presented by Knight Lightning                <>
<>                     February 11, 1989                      <>
<>                                                            <>
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
```

Beyond Bitnet lies the other wide area networks. We will discuss more about those networks in chapter four. Right now lets learn how to communicate with those other realms.

_

Mailing To Other Networks - Gateway Communications
~~~~~~~~~~~~~~~~~~~~~~~~~

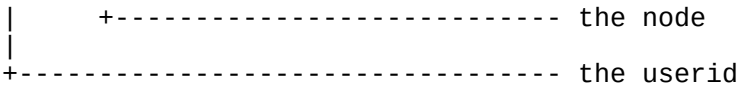
Bitnet, as you already know, is not the only computer network in the world. What you might be surprised to find out, however, is that when you have access to Bitnet you also have access to many other networks as well. Unfortunately, the methods for communicating with people in these other networks are not as simple as the ones described earlier.

Bitnet's links to other networks give you access to people and services you could not contact otherwise (or at least without great expense). This alone should make learning a bit about them worthwhile.

In chapter one of this series, I showed you how some Bitnet nodenames can be broken down into state abbreviations. To go a step further, try and think of Bitnet as a country and the links between the Bitnet nodes as highways. Another network (or country in this example) is connected to our highway system
at one point, which is called a "gateway." These borders do not let interactive messages or files through; only mail is allowed past the gateway.

The people in these other networks have addresses just like yours, but you will
need to specify something extra in order to get mail to them. A userid@node address is not enough, because that does not tell the Bitnet mail software what
network that node is in. Therefore, we can extend the network address with a code that identifies the destination network. In this example, the destination
network is ARPAnet (a network I'm sure you have heard much about), the code for
which is ARPA.

```
TARAN@MSP-BBS.ARPA
+---- +------ +---
|     |       |
|     |       +-------------------- the network
|     |
```
~~~~~~~~~~~~~~~~~~~~~~~~~



That is about as simple as an address from another network gets. Generally they are much more complex. Because of the variety of networks there can be no example which will show you what a "typical" address might be. However, you should not have to let it worry you too much. If someone tells you that his network address is C483307@UMCVMB.MISSOURI.EDU, just use it like that with your mail software. As long as you understand that the mail is going to another network and that the transit time may be longer than usual (although in many cases I have found that mail going to EDU addresses is delivered much faster than Bitnet mail) you should not have many problems.

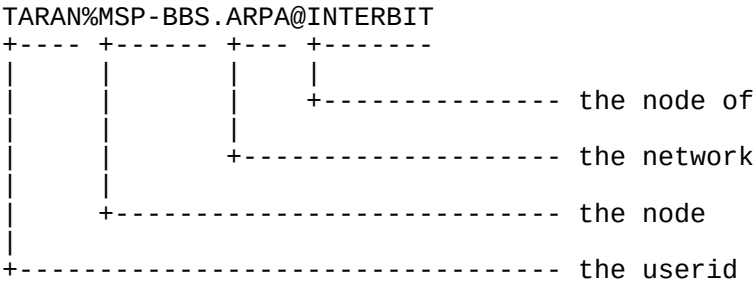
More On Gateways

I introduced the gateways in the previous section, but didn't get into too much detail. This is because the subject can get more than a little complex at times. Actually, understanding gateways isn't difficult at all, but interpreting network addresses that use them can be.

In the previous example, an address for someone in another network looked like this:

```
TARAN@MSP-BBS.ARPA
```

The ".ARPA" in the address tells your networking software that your letter should go to someone in another network. What you might not realize is that your networking software "knows" that the address for the gateway to ARPA may be at, say INTERBIT. It might extend the address to look something like this:



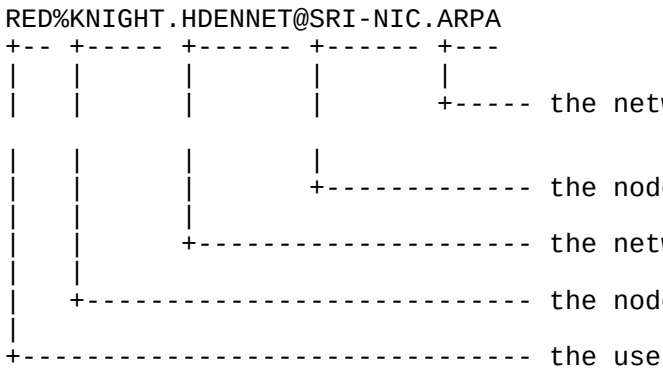
The gateway is a server machine (userid@node) that transfers files between the two networks. In this case, it is ARPA@INTERBIT. Note that the "%" replaces the "@" from the previous example. This is because Bitnet networking software cannot handle addresses with more than one AT sign (@). When your mail gets to the gateway, the "@INTERBIT" would be stripped off, and the "%" would be turned back into a "@".

Ok, so now you are asking, "If this is so automatic, why do you need to know this?" In many cases your networking software is not smart enough to know that the gateway for SCONNET is at STLMOVM. If this is the case, you have to type

out the whole address with all of the interesting special characters.

For example, sometimes, you may have to change the addresses around somewhat. Let's say I'm talking to Lex Luthor one day and he tells me his address is "lex@plover.COM". I have found that an address like "lex@plover.COM" would actually be mailed to as "plover!lex@RUTGERS.EDU". Now this is just a specific
example of how it works from my particular system and other systems (not to mention networks) will work differently (this is a guide for people using Bitnet). The COM (Commercial) addresses are not recognized by the mailer at UMCVMB and so I have to route them through Rutgers University. In chapter four, I will discuss some of the other networks that are interconnected.

In many cases, a gateway to a network may be in another network. In this example, we are sending mail to RED at node KNIGHT in HDENNET. The gateway to the network is in, say, ARPAnet. Our networking software is smart enough to know where ARPA gateway is, so the address might look something like this:



As you can see, these addresses can get pretty long and difficult to type. Perhaps the only consolation is that your address probably looks just as bad to
the people in the destination network.

Foundations Abound

Just as there are servers and services in Bitnet, there are similar counterparts in the other networks as well. There are many electronic digests and servers that are similar to Bitnet servers available on several of the other networks.

Gateways To Non-Standard Networks - Intermail

Intermail is perhaps the most interesting exception to standard gateways. It's
better to just show you what I mean rather than try to really technically describe the process. With Intermail, you can access networks you probably never thought were accessible.

I have included the instructions for using the Intermail system for transmitting computer mail between users in the MCI-Mail system, the GTE Telemail system, the Compmail/Dialcom 164 system, and the NFS-Mail/Dialcom 157 system to the ARPA-Mail system. The Intermail system may be used in either direction.

Mail to be sent to MCI Mail, GTE Telemail, Compmail, or NSF-Mail is sent to the
"Intermail" mailbox on the local mail system. The Intermail system operates by
having a program service mailboxes in both the local and the destination mail
systems. When the right information is supplied at the beginning of a message,
the program forwards those messages into the other mail system.

In order for a message to be delivered to a mailbox in another mail system,
forwarding information must be included at the beginning of the text of each
message. This forwarding information tells the mail forwarding program which
mail system to forward the message to, and which mailboxes to send it to. This
information is in the form:

```
      Forward: <mail system>
      To: <user mailbox>
      <blank line>
```

The syntax allowed on the "To:" line is that of the system being forwarded
into. In ARPA-Mail it is also possible to send to a list of CC recipients in
any of the mail gateway systems. See the examples for further details.

In either direction, the local Subject field of the message to Intermail is
used as the Subject field of the message delivered in the other mail system.

Sending To Non-Standard Networks From Bitnet

In this direction, the Internet user must first send mail to the Intermail
mailbox on the ARPA-Internet. The address of "Intermail" is
"INTERMAIL@ISI.EDU". Next, the Mailbox forwarding information must be added at
the beginning of the text of each message. The names of the mailboxes are
MCI-MAIL, TELEMAIL (for GTE Telemail), COMPMAIL, and NSF-MAIL.

This information is in the form:

```
      Forward: <Type name of mailbox here>
      To: <a valid address on the system you're forwarding to>
      <blank line>
      <Message...>
```

Please Note: Although CompuServe (CIS), Telex, and FAX are accessible from
              MCI-Mail, the Intermail gateway does not support these services.
              However, there is a Bitnet-CompuServe gateway, but that will be
              discussed in the next section of this file.

Sending To Bitnet From Non-Standard Networks

Supposing that you have an account on MCI-Mail, GTE Telemail, Compmail, or
NSF-Mail and you would like to mail to someone on Bitnet, you would direct
your mail to one of the following addresses;

         "INTERMAIL" (actually MCI-ID "107-8239") in MCI-Mail,
         "INTERMAIL/USCISI" in GTE Telemail,
         "164:CMP00817" in Compmail/Dialcom 164, and

"157:NSF153" in NSF-Mail

Once you have done this, you actually type the following as the first two lines
in the mail:

```
Forward: ARPA
To: KNIGHT%MSPVMA.BITNET@CUNYVM.CUNY.EDU
<blank line>
<Message...>
```

In this example, KNIGHT is the userid and MSPVMA is the Bitnet node. CUNYVM.CUNY.EDU is the Internet gateway to ARPAnet. It's really just that simple.

- -

In case of questions or problems using Intermail, please send a message to Intermail-Request@ISI.EDU.

CompuServe
~~~~~~~~~~

The gateway is not yet live as of this writing. Testing on it has been delayed
somewhat because of high-priority projects inside CompuServe. However, it might be a safe bet that by the time you read this that the gateway will be complete.

The specific mechanism is that the gateway machine, 3B2/400 named Loquat, believes that it has a UUCP neighbor "compuserve" which polls it. In reality, the UUCP connection is a lie all around, but the gateway starts up on an hourly
basis, pokes through the UUCP queue, finds mail aimed at CompuServe, and creates script language on the fly suitable for a utility called Xcomm 2.2 to call CompuServe, download any waiting mail, and upload any queued mail.

Appropriate header hacking is done so that CompuServe looks like just another RFC-compliant entity on the Internet, and the Internet looks like yet another gatewayed system from the perspective of the CompuServe subscriber - a very minor modification to the usual syntax used in their mailer is needed, but this project has provided the impetus for them to generalize the mechanism, something they had apparently not needed before.

So that's where it stands. Loquat speaks with machines at Ohio State. At the moment, there is a problem preventing mail passage except between CompuServe and Ohio State, while they finish development and testing. Also, part of the header hacking done is to make CompuServe IDs look right on the Internet - the usual 7xxxx,yyy is a problem due to the presence of the ",".

Easynet
~~~~~~~

A mail gateway between Easynet and the UUCP network and DARPA Internet (including CSNET) is provided by the Western Research Laboratory in Palo Alto, California. Hopefully this service will provide improved communications between the DEC community and the Usenet and Internet communities.

Mailing From A Bitnet Site To An Easynet Node

To mail a message from an Internet site to an Easynet node (say MSPVAX), you type:

To: user%mspvax.dec.com@decwrl.dec.com

A few other forms are still accepted for backward compatibility, but their use is discouraged and they will not be described here.

Mailing From Easynet To Bitnet

For people on Easynet who would like to mail to people on Bitnet the following information may be of interest.

The gateway supports connection to Bitnet using a pseudo-domain syntax. These addresses are translated by the gateway to the proper form to address the gateway into Bitnet. To address users in Bitnet you type:

To: DECWRL::"user@host.bitnet"

(Example: To: DECWRL::KNIGHT@MSPVAX.BITNET)

Mailnet

The Bitnet-Mailnet Gateway no longer exists. EDUCOM's Mailnet Service was discontinued after June 30, 1987 in agreement with MIT.

DASnet

DASnet is one of the networks that is connected to AppleLink.

Sending to DASnet from Bitnet:

1. In the "TO" field, enter the DASnet gateway address: XB.DAS@STANFORD.BITNET
2. In the "SUBJECT" field, enter the DASnet user id (such as [1234AA]joe)

Example (0756AA is the DASnet address and randy is the user on that system):

To: XB.DAS@STANFORD.BITNET
Subject: [0756AA]randy

3. If you type a "!" after the address in the subject field, you can insert comments, but the subject line must be limited to 29 characters.
   Example; Subject: [0756AA]randy!Networks are cool

Sending to Bitnet from DASnet

1. In the "TO" field, enter the BITNET address followed by "@dasnet"
2. Use the "SUBJECT" field for comments.

Example:

To: knight@umcvmb.bitnet@dasnet#MSubject: Gateways

Don't be confused, there are two @s and a at the end.

Gateways Between Bitnet And Other Networks Not Previously Detailed
~~~~~~

"u" = UserId	"h" = Host (Node)	"d" = Node (Host)

To: CSNET Phonenet	<u>@<h>.csnet
To: JANET (Domains: U: uk)	<u>%<d>.U@ac.uk
To: EAN (Domains: E: cdn, dfn, etc.)	<u>@<d>.E
To: COSAC	<h>/<u>@france.csnet
To: Xerox Internet (Domains: R: A registry)	<u>.R@xerox.com
To: DEC's Easynet <*Detailed Earlier*>	<u>%<h>.dec.com@decwrl.dec.com
To: IBM's VNET	<u>@vnet
To: ACSNET (Domains: A: oz.au)	<u>%<d>.A@<g>
To: UUCP	h1!h2!<h>!<u>@psuvax1
To: JUNET (Domains: J: junet)	<u>%<d>.J@csnet-relay.csnet
To: JANET	<u>%U.<d>@ac.uk

- -

To: BITNET

From	
ARPA Internet	<u>%<h>.bitnet@cunyvm.cuny.edu
CSNET Phonenet	<u>%<h>.bitnet@relay.cs.net
JANET	<u>%<h>@uk.ac.rl.earn
EAN	<u>@<h>.bitnet
COSAC	adi/<u>%<h>.bitnet@relay.cs.net
ACSNET	<u>%<h>.bitnet@munnari.oz
UUCP	psuvax1!<h>.bitnet!<u>
JUNET	<u>@<h>.bitnet

Conclusion
~~~~~~~~~~

Now that you understand how to mail to the other networks by making use of the gateways, we will begin looking at the other networks themselves. As my greatest area of expertise is Bitnet, I will cover the other networks in less detail. If they interest you, I'm sure you will find a way to learn more about them. So read Chapter Four of The Future Transcendent Saga -- Frontiers.

:Knight Lightning

==Phrack Inc.==

Volume Two, Issue 24, File 4 of 13

```
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
<>                                                              <>
<>                          Frontiers                           <>
<>                          ~~~~~~~~~                           <>
<>        Chapter Four of The Future Transcendent Saga          <>
<>                                                              <>
<>                 Beyond Bitnet Lies Infinity                  <>
<>                                                              <>
<>                Presented by Knight Lightning                 <>
<>                      February 12, 1989                       <>
<>                                                              <>
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
```

Welcome to the final chapter of The Future Transcendent Saga... or is it? Can there ever really be a final chapter to the future? In any case, I have collected information on some of the various other networks that you may comes across through your use of Bitnet. These listings are more of a summary than a detail guide (like Utopia was for Bitnet). However, I think you'll make good use of the information presented here. Much of the information in this file is based on examination of research conducted in July, 1987. Any errors due to the advancement in technology and the difference in time are apologized for.

The networks indexed in this file include the government agency networks ARPANET, MILNET, MFENET, and NSFnet; and the user-formed networks CSNET, HEANET, SPAN, TEXNET, UUCP, and USENET.

This file is not intended to be a hackers guide, but merely a directory of some of the networks.

One last thing to mention... the major top level domains on the Internet are:

```
     .EDU   Educational Institutions
     .COM   Commercial
     .GOV   Government
     .MIL   Military
     .ORG   Miscellaneous Orgainizations (that don't fit elsewhere)
```

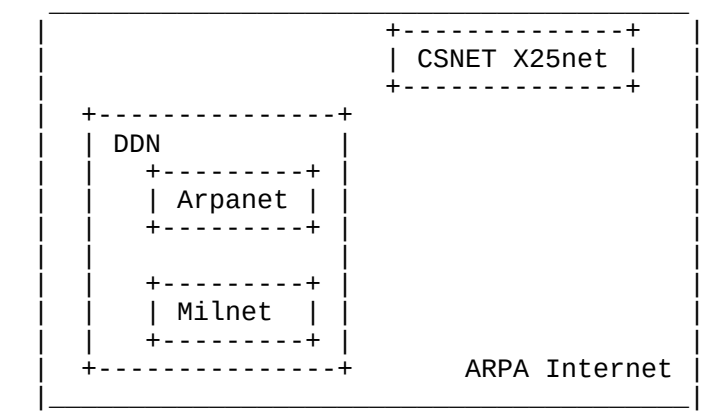
GOVERNMENT AGENCY NETWORKS
~~~~~~~~~~~~~~~~~~~~~~~~~~

ARPANET and MILNET

In 1969 the Defense Advanced Research Projects Agency (DARPA) began a research program to advance computer networking. The experimental packet-switched network that emerged was called ARPANET, and it allowed computers of different types to communicate efficiently. Using ARPANET technology, the Defense Data Network (DDN) was created in 1982 to encompass the existing ARPANET and other Department of Defense (DoD) computer networks. The DDN uses the DoD Internet Protocol Suite, including TCP/IP (Transmission Control Protocol/Internet Protocol) and associated application protocols.
~~~~~~~~~~~~~~~~~~~~~~~~~~

A splitting of the ARPANET was begun in 1983 and completed in 1984. The result
was two networks, an experimental research and development network called ARPANET, and a non-classified operational military network called MILNET. Gateways interconnect the two networks. The backbones of each of the networks consist of Packet Switched Nodes (PSNs), most of which are connected with 56 Kb
terrestrial lines. As of January 1987, the ARPANET had 46 PSNs, and MILNET had
117 PSNs in the U.S. and 33 in Europe and the Pacific.

While ARPANET and MILNET make up part of the DDN, the DDN and other networks works which share the same protocols make up the ARPA Internet. CSNET X25net, which uses the TCP/IP protocols interfaced to the public X.25 network, is an example of a network which is part of the ARPA Internet and is not a part of the DDN.



Policy, access control and funding for the ARPANET are provided by DARPA's Information Processing Techniques Office (IPTO). ARPANET and MILNET operation and management are provided by the Defense Communications Agency's DDN Program Management Office (DDN PMO).

Use of the ARPANET is limited to users engaged in experimental research for
the
U.S. government, or government-sponsored research at universities. Because it is not meant to compete with commercial networks, it is not intended for operational communication needs or use by the general public.

Services available on ARPANET and MILNET include remote login, file transfer, mail, time, and date. Mail addressing on both of the networks is of the form user@domain, where domain refers to a full qualified domain name composed of a string of one or more subdomains separated by a period, ending with a top-level
domain. Examples of top-level domains: edu, com, gov, mil, net, org, jp, au, uk. Examples of fully qualified domain names: kentarus.cc.utexas.edu, relay.cs.net, icot.jp.

The DDN funds a Network Information Center (NIC), located at SRI International in Menlo Park, California, which provides user services to DDN users via electronic mail (NIC@SRI-NIC.ARPA), telephone (800-235-3155) and U.S. mail: DDN Network Information Center, SRI International, Room EJ291, 333 Ravenswood Avenue, Menlo Park, CA 94025. The telephone service is available Monday through
Friday, 7a.m to 4p.m., Pacific time.

Much information is also available on-line on SRI-NIC.ARPA, via telnet or

anonymous ftp (login "anonymous", password "guest"). The file NETINFO:NETINFO-INDEX.TXT contains an index of these on-line files.

MFENET

MFEnet is the Department of Energy's (DOE) magnetic fusion energy research network. It was established in the mid-1970's to support access to the MFE Cray 1 supercomputer at the Lawrence Livermore National Laboratory. The network uses 56-kbs satellite links, and is designed to provide terminal access to the Cray time-sharing system (CTSS), also developed at the Lawrence Livermore Laboratory. The network currently supports access to Cray 1, Cray X-MP/2, Cray 2, and Cyber 205 supercomputers. The network uses special-purpose networking software developed at Livermore, and, in addition to terminal access, provides file transfer, remote output queuing, and electronic mail, and includes some specialized application procedures supporting interactive graphics terminals and local personal computer (PC)-based editing. Access to the network is in general restricted to DOE-funded researchers. A couple of years ago, the network was expanded to include the DOE-funded supercomputer at Florida State University. MFEnet is funded by DOE and managed by Livermore.

MFEnet has been successful in supporting DOE supercomputer users. However, the specialized nature of the communications protocols is now creating difficulties for researchers who need advanced graphics workstations that use the UNIX BSD 4.2 operating system and the TCP-IP protocols on LAN's. For these and other reasons, DOE is examining how best to migrate MFEnet to the TCP-IP, and later to the OSI, protocols.

The combination of the CTSS operating system and the MFEnet protocols creates an effective interactive computing environment for researchers using Cray supercomputers. For this reason, two of the new NSF national supercomputer centers -- San Diego (SDSC) and Illinois -- have chosen the CTSS operating system. In SDSC's case, the MFENET protocols have also been chosen to support the SDSC Consortium network. In Illinois case, a project to implement the TCP-IP protocols for the CTSS operating system has been funded by the NSFnet program, and these developments will be shared with SDSC (and with DOE) to provide a migration path for the SDSC Consortium network.

Mail can be sent to people on MFEnet by using this format;

user%site.MFENET@NMFEDD.ARPA

NSFNET

NSFnet began in 1986 as a communications network to facilitate access to NSF-funded national supercomputer centers. It is evolving into a general purpose internet for research and scientific information exchange. The network has a three-level component structure comprised of a backbone, several autonomously administered wide-area networks, and campus networks. The backbone includes the following supercomputer centers:

- National Center for Supercomputing Applications, University of Illinois, Urbana (UIUC)

- Cornell National Supercomputer Facility, Cornell University (Cornell)
- John von Neumann National Supercomputer Center, Princeton, New Jersey (JVNC)
- San Diego Supercomputer Center, University of California, San Diego (SDSC)
- Pittsburgh Supercomputer Center (Westinghouse Electric Corp, Carnegie-Mellon University, University of Pittsburgh)
- Scientific Computing Division of the National Center for Atmospheric Research, Boulder, Colorado (NCAR)

Upper layer protocols in use on the NSFnet backbone are the TCP/IP protocols. The backbone became operational in July of 1986. It was composed of seven 56 kps links between six IP gateways. These gateways are LSI 11/73 systems. An upgrade to T1 links (1.544 Mps) was established in the latter part of 1987. There are plans to adopt the OSI networking protocols as the software becomes available.

NSF-funded component networks include:

BARRNET - California's Bay Area Regional Research Network
MERIT - Michigan Educational Research Network
MIDNET - Midwest Network
NORTHWESTNET - Northwestern states
NYSERNET - New York State Educational and Research Network
SESQUINET - Texas Sesquicentennial Network
SURANET - Southeastern Universities Research Association Network
WESTNET - Southwestern states
JVNCNET - consortium network of JVNC
SDSCNET - consortium network of SDSC
PSCAAnet - consortium network of the Pittsburgh Supercomputer Center

Some of the component networks preceded NSFnet, and some of them have just recently been established. Each of the component networks is connected to the backbone. Information about the status of any NSFnet component network is available from the NSFnet Network Service Center (NNSC). Monthly reports on the status of the backbone and component networks are also available on-line through the CSNET Info-Server. Send a message to info-server@sh.cs.net with the following message body:

REQUEST: NSFNET
TOPIC: NSFNET-HELP
REQUEST:END

These reports may also be retrieved by anonymous ftp (login "anonymous", password "guest") from sh.cs.net, in the directory "nsfnet." [FTP stands for File Transfer Protocol]

Other autonomous networks connected to the NSFnet backbone include ARPANET, BITNET, CSNET, and USAN (the University Satellite Network of the National Center for Atmospheric Research).

Interesting projects associated with NSFnet include implementation of the gated
routing daemon which handles the RIP, EGP and HELLO routing protocols and runs on 4.3BSD, Ultrix TM, GOULD UTX/32 TM, SunOS and VMS TM (Cornell University Theory Center); implementation of TCP/IP for the CTSS operating system supporting TELNET and FTP (University of Illinois); and a satellite experiment providing 56 kps links between distant ethernets using Vitalink technology (NCAR).

Management of the NSFnet is in an interim form with duties shared among The

University of Illinois, Cornell University, the University of Southern California Information Sciences Institute, and University Corporation for Atmospheric Research. The NSFnet project is administered by the Division of Network and Communications Research and Infrastructure, which is part of the Computer and Information Science and Engineering Directorate at NSF.

Further information is available from the NSFnet Network Service Center (NNSC),
BBN Laboratories Inc., 10 Moulton Street, Cambridge, MA 02238. Assistance can also be obtained by electronic mail to nnsc@nnsc.nsf.net, or by calling 617-497-3400. The NNSC is run by Bolt, Beranek and Newman, and is an NSF-funded project of the University Corporation for Atmospheric Research.

USER-FORMED NETWORKS

CSNET

In 1980 a proposal was presented to the National Science Foundation to fund a computer science research network to link any university, commercial or government organizations involved in research or advanced development in computer science and computer engineering. NSF provided funding for the period
for 1981 to 1985, and CSNET was established. This single logical network today
connects approximately 200 computers on three physical networks. These component physical networks are Phonenet, X25net and a subset of the ARPANET. Phonenet is a store-and-forward network using MMDF software over public telephone lines to provide electronic mail service. X25net utilizes the public
X.25 packet switched network Telenet, interfaced with TCP/IP, to provide electronic mail, file transfer and remote login. Some ARPANET hosts are also members of CSNET. The computers linked by CSNET are in the U.S., Europe, Canada, Israel, Korea and Japan. Addressing in CSNET is in the ARPA Internet domain style.

In 1981 a contract was arranged with Bolt, Beranek and Newman, Inc. to provide information, user and technical services for CSNET, and the CSNET Coordination and Information Center (CIC) was established. The CIC handles the daily management of the network, and oversight is provided by the CSNET Executive Committee. The network is supported by membership fees.

The CIC maintains a User Name Server database, which is accessible through the ns command on CSNET hosts running appropriate software, or by telnet to the CSNET service host, sh.cs.net (login "ns", no password required). There is also much information available via anonymous ftp to sh.cs.net (login "anonymous", password "guest"), particularly in the directory "info." The Info
Server also provides a means for retrieving this information. To utilize the Info Server, send mail to infoserver@sh.cs.net with the following lines in the message body:

```
REQUEST:  INFO
TOPIC:  HELP
REQUEST:  END
```

The on-line information includes software, policy documents, information on other networks, site lists and mailing list archives.

CSNET Foreign Affiliates and their gateways are:

CDNNET -- Canadian Academic Network, University of British Columbia.

SDN -- System Development Network (SDN) is an R&D computer network, consisting of computers of R&D communities in Republic of Korea, with a gateway at KAIST, Korea Advanced Institute of Science and Technology, Seoul. It has mail connection to CSNET/Internet, USENET/EUNET/UUCP Net and Pacific countries like Australia, Indonesia, Hong Kong, Singapore and Japan.

SUNET -- Swedish University Network, Chambers University of Technology, Gothenburg.

CHUNET -- Swiss University Network, ETH-Zentrum, Zurich.

Inria -- French University Network, Institute National de Recherce en Informatique, Rocquencourt.

DFN -- Deutches Forschungsnetz, GWD-Gesellschaft fuer Mathematick und Datenvararbiten, Schloss Birlinghoven, St. Augustin.

JUNET -- Japanese University Network, University of Tokyo.

Finnish University Network, Helsinki University, Helsinki.

AC.UK -- Academic Community, United Kingdom, University College, London.

ACSNET -- A UUCP-based academic network in Australia, University of Melbourne.

New Zealand Academic Network, Waikato University, Hamilton.

Israeli Academic Network, Hebrew University of Jerusalem.

For more information contact CSNET CIC, BBN Laboratories Inc., 10 Moulton Street, Cambridge, MA 02238, or send electronic mail to cic@sh.cs.net (cic@csnet-sh.arpa). A 24-hour hotline is also available, (617) 497-2777.

HEANET

HEAnet is a network linking the Universities and National Institutes for Higher
Education in the Republic of Ireland. The following institutions belong to HEANET:

NIHED: National Institute for Higher Education, Dublin
NIHEL: National Institute for Higher Education, Limerick
MAY: St. Patrick's College, Maynooth
TCD: Trinity College, Dublin
UCC: University College, Cork
UCD: University College, Dublin
UCG: University College, Galway

The abbreviations on the left are used to form the network addresses for the hosts belonging to each institution. Addresses use the form:

host.institution.IE (for example VAX2.NIHED.IE)

HEANET is connected to EARN/Bitnet/Netnorth by a gateway at University College,
Dublin. Mail for HEANET should be sent as a BSMTP "job" to MAILER at IRLEARN.

SPANet

The Space Physics Analysis Network (SPAN) became operational in 1981, and was the result of a pilot project at Marshall Space Flight Center funded by NASA (Space Plasma Physics Branch, Office of Space Science). The network is a mission-independent data system testbed, intended to address problems of exchanging data (raw and processed), analysis software, graphic images and correspondence between researchers in several disciplines, including Solar-Terrestrial, Interplanetary and Planetary Physics, Astrophysics, Atmospherics, Oceans, Climate and Earth Science. A perception that multidisciplinary correlative research in solar-terrestrial physics would increase in the 1980's, that standards were lacking in scientific databases, and that support was required for the display of device independent graphic images, all motivated the establishment of SPAN. SPAN has therefore developed to facilitate space data analysis and address significant unresolved problems of scientific data exchange and correlation.

The Data Systems Users Working Group, formed in 1980, provides guidance and policy recommendations to SPAN. Daily operation of the network is performed by
a network and project manager, a project scientist, routing center managers, and managers at the local nodes.

SPAN nodes communicate using a variety of transmission media (fiber optics, coax, leased telephone lines) and lower layer protocols (ethernet, X.25, DDCMP), and nearly all SPAN hosts use the DECnetTM upper layer protocols. There
are plans to migrate to the emerging OSI protocols as software becomes available.

Currently SPAN connects over 1200 computers throughout the United States, Europe, Canada, and Japan (leading to all of the hacker related trouble on the network, such as the Mathias Speer incident). The network backbone in the United States consists of redundant 56 kps links between 5 DECnet routing centers:

1. NASA's Johnson Space Center (Houston, Texas)
2. NASA and Cal Tech's Jet Propulsion Laboratory (Pasadena, California)
3. NASA's Marshall Space Flight Center (Huntsville, Alabama)
4. NASA's Goddard Space Flight Center (Greenbelt, Maryland)
5. NASA's Ames Research Center (Moffett Field, California)

Tail circuits connect SPAN member institutions to the closest routing center, in most cases with leased lines at a minimum of 9.6 kps.

SPAN is gatewayed to CSNET, ARPANET, BITNET, GTE Telenet, JANET and the NASA Packet Switched System (NPSS). SPAN is joined to TEXNET, HEPnet and other DECnetTM wide area networks. Services available to SPAN nodes include electronic mail, remote file transfer and remote login.

Additional information is available from the SPAN Network Information Center (SPAN-NIC) located at the National Space Science Data Center, NASA Goddard Space Flight Center, Greenbelt, Maryland 20771. Assistance is also available by electronic mail at NSSDCA::SPAN_NIC_MGR.

_

TEXNET

Most of TEXNET became operational in 1986, although pieces of this network existed earlier. The purpose of the network is to link computers at Texas universities which run the DECnetTM upper layer protocols. Lower layer protocols in use on the network are ethernet (IEEE 802.3) and DDCMP (Digital Data Communication Message Protocol). TEXNET currently connects over 450 machines in 14 cities. The network backbone consists of DECnetTM routers, and some synchronous links, connected via leased lines. 9600 bps and 56 Kbps lines
are used.

Gateways exist from TEXNET to SPAN, BITNET and the ARPA Internet. Services provided include electronic mail, file transfer and remote login.

Operational and policy management of the network is by consensus of an informal
management group composed of managers from each member institution.

The following institutions are TEXNET members:

Baylor University
Houston Area Research Center
Pan American University
Sam Houston State University
Southwest Texas State University
Texas A & M University
University of Houston
University of Texas at Arlington
University of Texas at Austin
University of Texas at El Paso
University of Texas at Dallas
University of Texas at Permian Basin
University of Texas at San Antonio
University of Texas at Tyler
University of Texas Health Center at Tyler
University of Texas Health Science Center at Dallas
University of Texas Health Science Center at Houston
University of Texas Health Science Center at San Antonio
University of Texas Medical Branch Galveston
University of Texas System Cancer Center
University of Texas System Center for High Performance Computing
University of Texas Office of Land Management

_

UUCP and USEnet

The UUCP network was started in the 1970's to provide electronic mail and file transfer between UNIX systems. The network is a host-based store-and-forward network using dialup telephone circuits and operates by having each member site
dialup the next UUCP host computer and send and receive files and electronic mail messages. The network uses addresses based on the physical path established by this sequence of dialups connections. UUCP is open to any UNIX system which chooses to participate. There are "informal" electronic mail gateways between UUCP and ARPANET, BITNET, or CSNET, so that users of any of these networks can exchange electronic mail.

USENET is a UNIX news facility based on the UUCP network that provides a news bulletin board service. USEnet has both academic and commercial members and affiliates in Europe, Asia, and South America. Neither UUCP nor USENET has a central management; volunteers maintain and distribute the routing tables for the network. Each member site pays its own costs and agrees to carry traffic. Despite this reliance on mutual cooperation and anarchic management style, the network operates and provides a useful, if somewhat unreliable, and low-cost service to its members. Over the years the network has grown into a world-wide
network with thousands of computers participating.

"The Future Is Now"

==Phrack Inc.==

Volume Two, Issue 24, File 5 of 13

Control Office Administration Of Enhanced 911 Services For Special Services And Major Account Centers

By The Eavesdropper

March, 1988

Description of Service

The control office for Emergency 911 service is assigned in accordance with the existing standard guidelines to one of the following centers:

- Special Services Center (SSC)
- Major Accounts Center (MAC)
- Serving Test Center (STC)
- Toll Control Center (TCC)

The SSC/MAC designation is used in this document interchangeably for any of these four centers. The Special Services Centers (SSCs) or Major Account Centers (MACs) have been designated as the trouble reporting contact for all E911 customer (PSAP) reported troubles. Subscribers who have trouble on an E911 call will continue to contact local repair service (CRSAB) who will refer the trouble to the SSC/MAC, when appropriate.

Due to the critical nature of E911 service, the control and timely repair of troubles is demanded. As the primary E911 customer contact, the SSC/MAC is in the unique position to monitor the status of the trouble and insure its resolution.

System Overview

The number 911 is intended as a nationwide universal telephone number which provides the public with direct access to a Public Safety Answering Point (PSAP). A PSAP is also referred to as an Emergency Service Bureau (ESB). A PSAP is an agency or facility which is authorized by a municipality to receive and respond to police, fire and/or ambulance services. One or more attendants are located at the PSAP facilities to receive and handle calls of an emergency nature in accordance with the local municipal requirements.

An important advantage of E911 emergency service is improved (reduced) response times for emergency services. Also close coordination among agencies providing various emergency services is a valuable capability provided by E911 service.

1A ESS is used as the tandem office for the E911 network to route all 911 calls to the correct (primary) PSAP designated to serve the calling station. The E911 feature was developed primarily to provide routing to the correct PSAP for

all 911 calls. Selective routing allows a 911 call originated from a particular station located in a particular district, zone, or town, to be routed to the primary PSAP designated to serve that customer station regardless
of wire center boundaries. Thus, selective routing eliminates the problem of wire center boundaries not coinciding with district or other political boundaries.

The services available with the E911 feature include:

Forced Disconnect	Default Routing
Alternative Routing	Night Service
Selective Routing	Automatic Number Identification (ANI)
Selective Transfer	Automatic Location Identification (ALI)

Preservice/Installation Guidelines

When a contract for an E911 system has been signed, it is the responsibility of
Network Marketing to establish an implementation/cutover committee which should
include a representative from the SSC/MAC. Duties of the E911 Implementation Team include coordination of all phases of the E911 system deployment and the formation of an on-going E911 maintenance subcommittee.

Marketing is responsible for providing the following customer specific information to the SSC/MAC prior to the start of call through testing:

- All PSAP's (name, address, local contact)
- All PSAP circuit ID's
- 1004 911 service request including PSAP details on each PSAP (1004 Section K, L, M)
- Network configuration
- Any vendor information (name, telephone number, equipment)

The SSC/MAC needs to know if the equipment and sets at the PSAP are maintained by the BOCs, an independent company, or an outside vendor, or any combination. This information is then entered on the PSAP profile sheets and reviewed quarterly for changes, additions and deletions.

Marketing will secure the Major Account Number (MAN) and provide this number to
Corporate Communications so that the initial issue of the service orders carry the MAN and can be tracked by the SSC/MAC via CORDNET. PSAP circuits are official services by definition.

All service orders required for the installation of the E911 system should include the MAN assigned to the city/county which has purchased the system.

In accordance with the basic SSC/MAC strategy for provisioning, the SSC/MAC will be Overall Control Office (OCO) for all Node to PSAP circuits (official services) and any other services for this customer. Training must be scheduled
for all SSC/MAC involved personnel during the pre-service stage of the project.

The E911 Implementation Team will form the on-going maintenance subcommittee prior to the initial implementation of the E911 system. This sub-committee will establish post implementation quality assurance procedures to ensure that the E911 system continues to provide quality service to the customer.

Customer/Company training, trouble reporting interfaces for the customer, telephone company and any involved independent telephone companies needs to be addressed and implemented prior to E911 cutover. These functions can be best addressed by the formation of a sub-committee of the E911 Implementation Team to set up guidelines for and to secure service commitments of interfacing organizations. A SSC/MAC supervisor should chair this subcommittee and include
the following organizations:

1) Switching Control Center
   - E911 translations
   - Trunking
   - End office and Tandem office hardware/software
2) Recent Change Memory Administration Center
   - Daily RC update activity for TN/ESN translations
   - Processes validity errors and rejects
3) Line and Number Administration
   - Verification of TN/ESN translations
4) Special Service Center/Major Account Center
   - Single point of contact for all PSAP and Node to host troubles
   - Logs, tracks & statusing of all trouble reports
   - Trouble referral, follow up, and escalation
   - Customer notification of status and restoration
   - Analyzation of "chronic" troubles
   - Testing, installation and maintenance of E911 circuits
5) Installation and Maintenance (SSIM/I&M)
   - Repair and maintenance of PSAP equipment and Telco owned sets
6) Minicomputer Maintenance Operations Center
   - E911 circuit maintenance (where applicable)
7) Area Maintenance Engineer
   - Technical assistance on voice (CO-PSAP) network related E911 troubles

Maintenance Guidelines

The CCNC will test the Node circuit from the 202T at the Host site to the 202T at the Node site. Since Host to Node (CCNC to MMOC) circuits are official company services, the CCNC will refer all Node circuit troubles to the SSC/MAC.
The SSC/MAC is responsible for the testing and follow up to restoration of these circuit troubles.

Although Node to PSAP circuit are official services, the MMOC will refer PSAP circuit troubles to the appropriate SSC/MAC. The SSC/MAC is responsible for testing and follow up to restoration of PSAP circuit troubles.

The SSC/MAC will also receive reports from CRSAB/IMC(s) on subscriber 911 troubles when they are not line troubles. The SSC/MAC is responsible for testing and restoration of these troubles.

Maintenance responsibilities are as follows:

SCC*	Voice Network (ANI to PSAP) *SCC responsible for tandem switch
SSIM/I&M	PSAP Equipment (Modems, CIU's, sets)
Vendor	PSAP Equipment (when CPE)
SSC/MAC (EMNT)	PSAP to Node circuits, and tandem to PSAP voice circuits
MMOC	Node site (Modems, cables, etc)

Note: All above work groups are required to resolve troubles by interfacing with appropriate work groups for resolution.

The Switching Control Center (SCC) is responsible for E911/1AESS translations in tandem central offices. These translations route E911 calls, selective transfer, default routing, speed calling, etc., for each PSAP. The SCC is also
responsible for troubleshooting on the voice network (call originating to end office tandem equipment).

For example, ANI failures in the originating offices would be a responsibility of the SCC.

Recent Change Memory Administration Center (RCMAC) performs the daily tandem translation updates (recent change) for routing of individual telephone numbers.

Recent changes are generated from service order activity (new service, address changes, etc.) and compiled into a daily file by the E911 Center (ALI/DMS E911 Computer).

SSIM/I&M is responsible for the installation and repair of PSAP equipment. PSAP equipment includes ANI Controller, ALI Controller, data sets, cables, sets, and other peripheral equipment that is not vendor owned. SSIM/I&M is responsible for establishing maintenance test kits, complete with spare parts for PSAP maintenance. This includes test gear, data sets, and ANI/ALI Controller parts.

Special Services Center (SSC) or Major Account Center (MAC) serves as the trouble reporting contact for all (PSAP) troubles reported by customer. The SSC/MAC refers troubles to proper organizations for handling and tracks status of troubles, escalating when necessary. The SSC/MAC will close out troubles with customer. The SSC/MAC will analyze all troubles and tracks "chronic" PSAP
troubles.

Corporate Communications Network Center (CCNC) will test and refer troubles on all node to host circuits. All E911 circuits are classified as official company property.

The Minicomputer Maintenance Operations Center (MMOC) maintains the E911 (ALI/DMS) computer hardware at the Host site. This MMOC is also responsible for monitoring the system and reporting certain PSAP and system problems to the
local MMOC's, SCC's or SSC/MAC's. The MMOC personnel also operate software programs that maintain the TN data base under the direction of the E911 Center.
The maintenance of the NODE computer (the interface between the PSAP and the ALI/DMS computer) is a function of the MMOC at the NODE site. The MMOC's at the NODE sites may also be involved in the testing of NODE to Host circuits. The MMOC will also assist on Host to PSAP and data network related troubles not
resolved through standard trouble clearing procedures.

Installation And Maintenance Center (IMC) is responsible for referral of E911 subscriber troubles that are not subscriber line problems.

E911 Center - Performs the role of System Administration and is responsible for
overall operation of the E911 computer software. The E911 Center does A-Z trouble analysis and provides statistical information on the performance of the

system.

This analysis includes processing PSAP inquiries (trouble reports) and referral of network troubles. The E911 Center also performs daily processing of tandem recent change and provides information to the RCMAC for tandem input. The E911 Center is responsible for daily processing of the ALI/DMS computer data base and provides error files, etc. to the Customer Services department for investigation and correction. The E911 Center participates in all system implementations and on-going maintenance effort and assists in the development of procedures, training and education of information to all groups.

Any group receiving a 911 trouble from the SSC/MAC should close out the trouble with the SSC/MAC or provide a status if the trouble has been referred to another group. This will allow the SSC/MAC to provide a status back to the customer or escalate as appropriate.

Any group receiving a trouble from the Host site (MMOC or CCNC) should close the trouble back to that group.

The MMOC should notify the appropriate SSC/MAC when the Host, Node, or all Node circuits are down so that the SSC/MAC can reply to customer reports that may be called in by the PSAPs. This will eliminate duplicate reporting of troubles. On complete outages the MMOC will follow escalation procedures for a Node after two (2) hours and for a PSAP after four (4) hours. Additionally the MMOC will notify the appropriate SSC/MAC when the Host, Node, or all Node circuits are down.

The PSAP will call the SSC/MAC to report E911 troubles. The person reporting the E911 trouble may not have a circuit I.D. and will therefore report the PSAP name and address. Many PSAP troubles are not circuit specific. In those instances where the caller cannot provide a circuit I.D., the SSC/MAC will be required to determine the circuit I.D. using the PSAP profile. Under no circumstances will the SSC/MAC Center refuse to take the trouble. The E911 trouble should be handled as quickly as possible, with the SSC/MAC providing as much assistance as possible while taking the trouble report from the caller.

The SSC/MAC will screen/test the trouble to determine the appropriate handoff organization based on the following criteria:

PSAP equipment problem: SSIM/I&M
Circuit problem: SSC/MAC
Voice network problem: SCC (report trunk group number)
Problem affecting multiple PSAPs (No ALI report from all PSAPs): Contact the MMOC to check for NODE or Host computer problems before further testing.

The SSC/MAC will track the status of reported troubles and escalate as appropriate. The SSC/MAC will close out customer/company reports with the initiating contact. Groups with specific maintenance responsibilities, defined above, will investigate "chronic" troubles upon request from the SSC/MAC and the ongoing maintenance subcommittee.

All "out of service" E911 troubles are priority one type reports. One link down to a PSAP is considered a priority one trouble and should be handled as if
the PSAP was isolated.

The PSAP will report troubles with the ANI controller, ALI controller or set equipment to the SSC/MAC.

NO ANI: Where the PSAP reports NO ANI (digital display screen is blank) ask if
this condition exists on all screens and on all calls. It is important to differentiate between blank screens and screens displaying 911-00XX, or all zeroes.

When the PSAP reports all screens on all calls, ask if there is any voice contact with callers. If there is no voice contact the trouble should be referred to the SCC immediately since 911 calls are not getting through which may require alternate routing of calls to another PSAP.

When the PSAP reports this condition on all screens but not all calls and has voice contact with callers, the report should be referred to SSIM/I&M for dispatch. The SSC/MAC should verify with the SCC that ANI is pulsing before dispatching SSIM.

When the PSAP reports this condition on one screen for all calls (others work fine) the trouble should be referred to SSIM/I&M for dispatch, because the trouble is isolated to one piece of equipment at the customer premise.

An ANI failure (i.e. all zeroes) indicates that the ANI has not been received by the PSAP from the tandem office or was lost by the PSAP ANI controller. The
PSAP may receive "02" alarms which can be caused by the ANI controller logging more than three all zero failures on the same trunk. The PSAP has been instructed to report this condition to the SSC/MAC since it could indicate an equipment trouble at the PSAP which might be affecting all subscribers calling into the PSAP. When all zeroes are being received on all calls or "02" alarms continue, a tester should analyze the condition to determine the appropriate action to be taken. The tester must perform cooperative testing with the SCC when there appears to be a problem on the Tandem-PSAP trunks before requesting dispatch.

When an occasional all zero condition is reported, the SSC/MAC should dispatch SSIM/I&M to routine equipment on a "chronic" troublesweep.

The PSAPs are instructed to report incidental ANI failures to the BOC on a PSAP
inquiry trouble ticket (paper) that is sent to the Customer Services E911 group
and forwarded to E911 center when required. This usually involves only a particular telephone number and is not a condition that would require a report to the SSC/MAC. Multiple ANI failures which our from the same end office (XX denotes end office), indicate a hard trouble condition may exist in the end office or end office tandem trunks. The PSAP will report this type of condition to the SSC/MAC and the SSC/MAC should refer the report to the SCC responsible for the tandem office. NOTE: XX is the ESCO (Emergency Service Number) associated with the incoming 911 trunks into the tandem. It is important that the C/MAC tell the SCC what is displayed at the PSAP (i.e. 911-0011) which indicates to the SCC which end office is in trouble.

Note: It is essential that the PSAP fill out inquiry form on every ANI failure.

The PSAP will report a trouble any time an address is not received on an address display (screen blank) E911 call. (If a record is not in the 911 data base or an ANI failure is encountered, the screen will provide a display noticing such condition). The SSC/MAC should verify with the PSAP whether the NO ALI condition is on one screen or all screens.

When the condition is on one screen (other screens receive ALI information) the
SSC/MAC will request SSIM/I&M to dispatch.

If no screens are receiving ALI information, there is usually a circuit trouble
between the PSAP and the Host computer. The SSC/MAC should test the trouble and refer for restoral.

Note: If the SSC/MAC receives calls from multiple PSAP's, all of which are receiving NO ALI, there is a problem with the Node or Node to Host circuits or the Host computer itself. Before referring the trouble the SSC/MAC should call the MMOC to inquire if the Node or Host is in trouble.

Alarm conditions on the ANI controller digital display at the PSAP are to be reported by the PSAP's. These alarms can indicate various trouble conditions o
so the SSC/MAC should ask the PSAP if any portion of the E911 system is not functioning properly.

The SSC/MAC should verify with the PSAP attendant that the equipment's primary function is answering E911 calls. If it is, the SSC/MAC should request a dispatch SSIM/I&M. If the equipment is not primarily used for E911, then the SSC/MAC should advise PSAP to contact their CPE vendor.

Note: These troubles can be quite confusing when the PSAP has vendor equipment
mixed in with equipment that the BOC maintains. The Marketing representative should provide the SSC/MAC information concerning any unusual or exception items where the PSAP should contact their vendor. This information should be included in the PSAP profile sheets.

ANI or ALI controller down: When the host computer sees the PSAP equipment down and it does not come back up, the MMOC will report the trouble to the SSC/MAC; the equipment is down at the PSAP, a dispatch will be required.

PSAP link (circuit) down: The MMOC will provide the SSC/MAC with the circuit ID that the Host computer indicates in trouble. Although each PSAP has two circuits, when either circuit is down the condition must be treated as an emergency since failure of the second circuit will cause the PSAP to be isolated.

Any problems that the MMOC identifies from the Node location to the Host computer will be handled directly with the appropriate MMOC(s)/CCNC.

Note: The customer will call only when a problem is apparent to the PSAP. When only one circuit is down to the PSAP, the customer may not be aware
there is a trouble, even though there is one link down, notification should appear on the PSAP screen. Troubles called into the SSC/MAC from
the MMOC or other company employee should not be closed out by calling the PSAP since it may result in the customer responding that they do not

have a trouble. These reports can only be closed out by receiving information that the trouble was fixed and by checking with the company employee that reported the trouble. The MMOC personnel will be able to verify that the trouble has cleared by reviewing a printout from the host.

When the CRSAB receives a subscriber complaint (i.e., cannot dial 911) the RSA should obtain as much information as possible while the customer is on the line.

For example, what happened when the subscriber dialed 911? The report is automatically directed to the IMC for subscriber line testing. When no line trouble is found, the IMC will refer the trouble condition to the SSC/MAC. The
SSC/MAC will contact Customer Services E911 Group and verify that the subscriber should be able to call 911 and obtain the ESN. The SSC/MAC will verify the ESN via 2SCCS. When both verifications match, the SSC/MAC will refer the report to the SCC responsible for the 911 tandem office for investigation and resolution. The MAC is responsible for tracking the trouble and informing the IMC when it is resolved.

For more information, please refer to E911 Glossary of Terms.

==Phrack Inc.==

Volume Two, Issue 24, File 6 of 13

Glossary Terminology For Enhanced 911 Services

By The Eavesdropper

March, 1988

E911 - Enhanced 911: Features available include selective routing, selective transfer, fixed transfer, alternate routing, default routing, Automatic Number Display, Automatic Location Identification, night service, default routing, call detail record.

End Office - Telephone central office which provides dial tone to the subscriber calling 911. The "end office" provides ANI (Automatic Number Identification) to the tandem office.

Tandem Office - Telephone central office which serves as a tandem (or hub) for all 911 calls. Must be a 1AESS type of central office. The tandem office translations contain the TN/ESN relationships which route the 911 call to the proper SAP. The tandem office looks up the ANI (TN) that it receives from the end office and finds the ESN (routing information) which corresponds to a seven digit number ringing in at a PSAP.

PSAP - Public Safety Answering Point, usually the police, fire and/or rescue groups as determined by the local municipalities. A "ringin" will not have ANI or ALI capabilities, but just receives calls or transferred calls from another PSAP.

ESN - Emergency Service Number (XXX) that is assigned to the subscriber's telephone number in the tandem office translations The ESN represents a seven digit number by which the tandem office routes the call to the proper PSAP. PSAPs with ALI capabilities also receive a display of the ESN information which shows which police, fire and rescue agency serves the telephone number calling 911. An ESN is a unique combination of police, fire, and rescue service for purposes of routing the E911 call.

ANI - Automatic Number Identification corresponds to the subscriber's seven digit telephone number. The ANI displays at the PSAP on the digital ANI display console.

ALI - Automatic Location Identification provides for an address display of the subscriber calling 911. With ALI, the PSAP receives the ANI display and an ALI display on a screen. The ALI display includes the subscriber's address, community, state, type of service and if a business, the name of the business. The PSAP will also get a display of the associated ESN information (police, fire, rescue).

Selective Routing - The capability to route a call to the particular PSAP serving the address associated with the TN making the 911 call. Selective routing is achieved by building TN/ESN

translations in the tandem central office. These translations are driven by the E911 data base which assigns the ESN to each telephone number based on the customer's address. Service order activity keeps the E911 data base updated. The E911 data base, in turn, generates recent change to the tandem office (through the SCC or RCMAC) to update the TN/ESN translations in the tandem data base.

Selective Transfer - Provides the PSAP with the ability to transfer the incoming 911 call to a fire or rescue service for the particular number calling 911 by pushing one button for fire or rescue. For example, if an incoming 911 call was reporting a fire, the PSAP operator would push the fire button on the ANI console; the call would go back to the tandem office, do a lookup for the seven digit number associated with fire department, for the ESN assigned to the calling TN, and automatically route the call to that fire department. This differs from "fixed" transfer which routes every call to the same fire or rescue number whenever the fire or rescue button is pushed. The PSAP equipment is optioned to provide either fixed or selective transfer capabilities.

Alternate Routing - Alternate routing provides for a predetermined routing for 911 calls when the tandem office is unable to route the calls over the 911 trunks for a particular PSAP due to troubles or all trunks busy.

Default Routing - Provides for routing of 911 calls when there is an ANI failure. The call will be routed to the "default" ESN associated with the he NNX the caller is calling from. Default ESNs are preassigned in translations and are usually the predominant ESN for a given wire center.

Night Service - Night service works the same as alternate routing in that the calls coming into a given PSAP will automatically be routed to another preset PSAP when all trunks are made busy due to the PSAP closing down for the night.

Call Detail Record - When the 911 call is terminated by the PSAP operator, the ANI will automatically print-out on the teletypewriter located at the PSAP. The printout will contain the time the call came into the PSAP, the time it was picked up by an operator, the operator number, the time the call was transferred, if applicable, the time the call was terminated and the trunk group number associated with the call. Printouts of the ALI display are now also available, if the PSAP has purchased the required equipment.

ANI Failure - Failure of the end office to identify the call and provide the ANI (telephone number) to the tandem office; or, an ANI failure between the tandem office and the PSAP.

Misroute - Any condition that results in the 911 call going to the wrong PSAP. A call can be misrouted if the ESN and associated routing information are incorrect in the E911 data base and/or tandem data base. A call can also be misrouted if the call is an ANI failure,

which automatically default routes.

Anonymous Call - If a subscriber misdials and dials the seven digit number associated with the PSAP position, they will come in direct and ANI display as 911-0000 which will ALI as an anonymous call. The seven digit numbers associated with the PSAP positions are not published even to the PSAPs.

Spurious 911 Call - Occasionally, the PSAP will get a call that is not associated with a subscriber dialing 911 for an emergency. It could be a subscriber who has not dialed 911, but is dialing another number, or has just picked up their phone and was connected with the PSAP. These problems are equipment related, particularly when the calls originate from electromechanical or step by step offices, and are reported by the E911 Center to Network Operations upon receipt of the PSAP inquiry reporting the trouble. The PSAP may get a call and no one is there; if they call the number back, the number may be disconnected or no one home.

Again these are network troubles and must be investigated. Cordless telephones can also generate "spurious" calls in to the PSAPs. Generally, the PSAP will hear conversation on the line, but the subscribers are not calling 911. The PSAP may report spurious calls to to repair if they become bothersome, for example, the same number ringing in continually.

No Displays - A condition where the PSAP ALI display screen is blank. This type of trouble should be reported immediately to the SSC/MAC. If all screens at the PSAP are blank, it is an indication that the problem is in the circuits from the PSAP to the E911 computer. If more than one PSAP is experiencing no display, it may be a problem with the Node computer or the E911 computer. The SSC/MAC should contact the MMOC to determine the health of the HOST computer.

Record Not Found - If the host computer is unable to do a look up on a given ANI request from the PSAP, it will forward a Record Not Found message to the PSA ALI screen. This is caused by service order activity for a given subscriber not being processed into the E911 data base, or HOST computer system problems whereby the record cannot be accessed at that point in time.

No ANI - This condition means the PSAP received a call, but no telephone number displayed on the ANI console. The PSAP should report this condition immediately to the SSC/MAC.

PSAP Not Receiving Calls - If a PSAP cannot receive calls or request retrievals from the E911 host computer, i.e., cable cut, the calls into that PSAP must be rerouted to another PSAP. The Switching Control Center must be notified to reroute the calls in the tandem office E911 translations.

MSAG - Master Street Address Guide. The MSAG ledgers are controlled by the

municipality which has purchased the E911 ALI service, in that they assign which police, fire or rescue agency will serve a given street and number range. They do this by assigning an ESN to each street range, odd, even, community that is populated in the county or municipality served. These MSAGs are then used as a filter for service order activity into the E911 computer data base to assign ESNs to individual TN records. This insures that each customer will be routed to the correct agency for their particular address. In a non-ALI County, TAR codes are used by the Telephone company to assign ESNs to service conductivity and the County does not control the ESN assignment. TAR codes represent the taxing authority for the given subscriber which should correspond to their police, fire and rescue agencies. The MG method, of course, is more accurate because it is using the actual service address of the customer to route the call and provides the county with more flexibility in assigning fire and rescue district, etc.

The Customer Services E911 Group maintains the E911 computer data base and interfaces with the County (customer) on all MSAG or data base activity.

==Phrack Inc.==

Volume Two, Issue 24, File 7 of 13

```
()()()()()()()()()()()()()()()()()()()()()()()()
()                                            ()
()          Advanced Bitnet Procedures        ()
()                                            ()
()                     by                     ()
()                                            ()
()           VAXBusters International         ()
()                                            ()
()()()()()()()()()()()()()()()()()()()()()()()()
```

Greetings! I have taken the time to write up a file about some of the more complex operations on Bitnet. I hope you enjoy it!   :-)

- -

You can send multiple messages to one user@node under VAX/VMS & JNET by just typing;

```
$ SEND/REMOTE <host> <user>
```

This will collect messages from the terminal until an empty line or CTRL-Z is entered.

Under Unix, the UREP package is popular to connect Unix boxes to Bitnet. The important user commands are as follows:

Messages
~~~~~~~~
netwrite user@host

Send one or more messages to the specified Bitnet user. Netwrite reads messages from it's standard input until an EOF is reached. If called from a terminal, netwrite will terminate on an empty line as well.

When you receive Bitnet messages on a Unix host, UREP looks for an executable file named .exwrite in your home directory. If it doesn't find such a file, the message is simply spit on your terminal. If .exwrite is present, UREP executes this program (which can be a shell script) with five parameters:

```
<To System> <To User> <From System> <From User> <Tty>
```

The <Tty> parameter tells the terminal to which UREP wanted to send the message. UREP then feeds the messages to .exwrite as standard input. The format of standard input is as follows:

```
<count (1 byte)><message (<count> bytes)>
```

To display these messages you need to have a "C" program, since a shell script is not capable of handling single bytes painlessly. I included my exwrite.c at the end of this file for a start.

Typically, .exwrite is used to log all incoming Bitnet messages. You can of
~~~~~~~~

course blow it up to send messages back to the sender when you're out to lunch,
etc. BTW, .exwrite is called with the user ID of the receiving user, so it's no
real security hole.

File Transfer

netcopy user@host [options]

Copy a file to the specified Bitnet user. The most important option is "name=<fname>.<ftype>", with which you can specify the file name to be used at the recipient's machine. More details are in the manual page.

When you receive Bitnet files on a Unix machine running UREP, they will be placed in your home directory under the name ":<fname>.<ftype>". These files are in NETDATA format, and they have to be converted to ASCII text files when you want to use them under Unix. This can be done with the command;

netdata [<input_file> [<output_file>]]

When <input_file> is unspecified, standard input is used. If <output_file> is unspecified, standard output is used.

Bitnet Commands

Though Bitnet has no remote login capability, you can execute a (restricted) set of commands on remote hosts. These commands can be used to query node status, lists of logged-on users, time and some other things.

This works as follows:

```
JNET:   $ SEND/COMMAND <host> [ <command> ]
UREP:   % netexec <host> [ <command> ]
CMS:    SMSG <server> CMD <host> <command>
```

The <server> under CMS is the Bitnet control process. In Europe, it is normally called "EARN." In the USA, it could be "BITNET" or maybe "RSCS." You're on your own here.

The <host> is the Bitnet host name which you want to execute the <command>. With JNET and UREP, you will be asked for multiple commands when you leave the <command> field empty. Again, input is terminated with EOF or an empty line.

I have found the following commands useful in daily life:

CPQ N	Get a list of the users currently logged in at the <host>. This command is supposed to exist on every Bitnet host, but some system managers like to restrict it for security reasons. On JNET and UREP hosts, FINGER performs a similar, but more elaborate function.
CPQ T	Make <host> tell you the current time at it's location.
Q <otherhost>	Make <host> tell you what the next hop to <otherhost> is. This is useful when you're interested in the network topology.

```
        Q <ohost> A     This makes <host> tell you what file is currently
                        active (being transmitted) for <ohost>.  This only
                        works for machines which are directly connected to
                        <host>.

        Q <ohost> Q     This makes <host> show you the queue of files
currently
                        waiting for transmission to <ohost>.  This is useful
                        when you want to trace some file which you sent to the
                        network.

        Q SYS           This makes <host> tell you about the RSCS links it
has.

Unfortunately, MVS-Hosts don't understand any of these commands, but simply
give an error message.  You can recognize these things by the string "HASP"
somewhere in the error message.

        Enjoy !

exwrite.c For Unix Hosts Running UREP
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

<-- cut here -->
/* exwrite.c - formatter for UREP rscs messages                          */

include <stdio.h>
include <sysexits.h>
include <pwd.h>
include <ctype.h>

main(argc, argv)

        int             argc;
        char            *argv[];
       struct  passwd  *pw;
        char            fname[255];
        FILE            *term;
        FILE            *log;
        int             count;
        char            buf[1024];
        char            *from_user;
        char            *from_host;
        char            *to_user;
        char            *to_host;
        char            *to_tty;
        char            *home_dir = "/tmp";

        if (argc != 6)
                fprintf(stderr, "%s: Invalid arguments\n", argv[0]);
                exit(EX_USAGE);


        /* initialise variables                                          */
        to_host = argv[1];
        to_user = argv[2];
        from_host = argv[3];
        from_user = argv[4];
        to_tty = argv[5];
```

```
        /* convert the receiving user to lowercase.  Under Unix, all    *
         * user names normally are lower case, and we need a valid      *
         * user name to determine the home directory                    */
        for (; *to_user; to_user++)
                *to_user = tolower(*to_user);
        to_user = argv[2];

        /* get the home directory of the receiving user                 */
        if (pw = getpwnam(to_user))
                home_dir = pw->pw_dir;

        /* open the terminal, exit if the open fails                    */
        sprintf(fname, "/dev/%s", to_tty);
        if (!(term = fopen(fname, "w")))
                exit(EX_OSERR);

        /* open the rscs log file                                       */
        sprintf(fname, "%s/.rscslog", home_dir);
        log = fopen(fname, "a");

        /* if the message is not coming from the relay, write the       *
         * sending user and host name to the specified terminal         */
        if (strcmp(from_user, "RELAY"))
                fprintf(term, "From %s@%s:\r\n", from_user, from_host);

        /* read in the RSCS messages and send them to the terminal      *
         * and to the logfile if it has been opened.                    *
         * In the log file, all lines are preceded by the sending user  *
         * and host name.                                               */
        while ((count = getchar()) != EOF)
                if ((count = fread(buf, 1, count, stdin)) > 0)
                        fwrite(buf, 1, count, term);
                        fprintf(term, "\r\n");
                        if (log)
                                fprintf(log, "%s@%s: ", from_user, from_host);
                                fwrite(buf, 1, count, log);
                                fprintf(log, "\n");



        exit(EX_OK);
```

_

==Phrack Inc.==

Volume Two, Issue 24, File 8 of 13

Special Area Codes

by >Unknown User<

January 3, 1989

Greetings! I have compiled information about the SACs for your edification; these include 700, 800, and 900.

Most telephone users from the United States are quite familiar with 800 service: A number that they dial and incur NO charge (not even message units in most areas).

Then there is 900 service, which is what most people perceive as 'value added,'
i.e. you pay more for the information than for the transport of the call. These vary typically from 35 cents to a few dollars for either a timed service,
or a 'as long as you like' duration-sensitive service. There are two sub-species of 900 service: AT&T and "everybody else."

Finally, there is 700 service, which many people remember as Alliance Teleconferencing. This is the third "canonical" SAC. With few limitations, this SAC is given over to the IEC entirely.

Let's look at these in more detail.

800 Service

800 service is offered by various IECs. Each NXX in the 800 SAC is assigned to
a given carrier, who is responsible for assigning numbers from that block to customers, and providing 10 digit translation.

The carrier must have Feature Group D presence for originating calls from the originating exchange (either direct, or through an access tandem).

In the future, when CCIS becomes wide-spread, a query will be made in the database [Who gets 1-800-985-1234?] and the call will be routed appropriately. To clarify: Now the carrier is determined by the NNX. In the future, the carrier will be determined by the entire 7 digits.

A similar situation exists with 900 service. Each carrier can reserve NXXs from BellCore (the people who among a zillion other tasks are in charge of handing out prefixes and area codes). They're not cheap! To get the actual number is free (there are qualifications that I don't deal with), but to get it
'turned on' in a LATA costs you money, depending on:

(1) How many prefixes you're getting,
(2) Whether it's 800 or 900 service; and,

(3) How many Tandems/End Offices are in the LATA.

It requires a discrete amount of labor for EACH office, because EACH routing table must be modified. However, I will be discussing 900 Service in more detail later in this file.

When you, as Joe Customer, dial 1-800-222-1234 (made up number, please don't bother them) it will initiate the following sequence:

1. If you are in an Electronic Office (DMS-100, DMS-200, 1A ESS, 5 ESS) the 800-222 will be translated to "AT&T" and will search for an opening in a trunk group marked for 800 origination. Should none be found, bump to step 3.

2. If you are in a non-electronic office (SxS, XB, and some flavors of ESS), it will go to the access tandem that your office 'homes' on, where 800-222 will be translated to "AT&T."

   Note: If at this point, the number doesn't have a translation, you will get a "lose" recording from the CO.

3. Find a trunk in a trunk group marked for 800 origination. Should none be found, give the customer a recording "Due to network congestion, your 800 call could not be completed" or die, or whatever. (Depends on phase of moon, etc.)

4. The end office will the send the following pulse-stream (in MF):
   KP + II + 3/10D + ST + KP + 800 222 1234 + ST

   Note: This is a simplification; there are some fine points of ANI spills that are beyond the scope of this file.

   II = 2 information digits. Typical values are:

   00 normal ANI .. 10 digits follow
   01 ONI line ... NPA follows
   02 ANI failure ... NPA follows

   3/10D = 3 or 10 digits. Either the NPA, or the entire 10 digit number. KP and ST are control tones.

5. The carrier receives all of this (and probably throws the ANI into the bit bucket) and translates the 800 number to what's called a PTN, or Plant Test Number (for example, 617-555-9111). Then, the call is routed AS IF the customer had dialed that 10 digit number. Of course, the billing data is marked as an 800 call, so the subscriber receiving the call pays the appropriate amount.

Of the 800 possible NXXs, 409 are currently assigned. A long-distance carrier can get one 800 and four 900 numbers just for the paperwork. But to get more than that, you have to show that you're 70% full now, and demonstrate a real need for the capacity.

I have included the entire 800-NXX to long-distance carrier translation table. Note that not every NXX is valid in every area.

- -

Revised 800/OCN Translation Table
Effective October 10, 1988

221 ATX	222 ATX	223 ATX	224 LDL	225 ATX
226 MIC	227 ATX	228 ATX	229 TDX	230 NTK
231 ATX	232 ATX	233 ATX	234 MCI	235 ATX
236 SCH	237 ATX	238 ATX	239 DLT	240 SIR
241 ATX	242 ATX	243 ATX	244 ---	245 ATX
246 ---	247 ATX	248 ATX	249 ---	250 ---
251 ATX	252 ATX	253 ATX	254 TTU	255 ATX
256 LSI	257 ATX	258 ATX	259 ---	260 ---
261 SCH	262 ATX	263 CAN	264 ICT	265 CAN
266 CSY	267 CAN	268 CAN	269 FDG	270 ---
271 ---	272 ATX	273 ---	274 MCI	275 ITT
276 ONE	277 SNT	278 ---	279 MAL	280 ADG
281 ---	282 ATX	283 MCI	284 MCI	285 ---
286 ---	287 ---	288 MCI	289 MCI	290 ---
291 ---	292 ATX	293 PRO	294 ---	295 ---
296 ---	297 ARE	298 ---	299 CYT	

321 ATX	322 ATX	323 ATX	324 HNI	325 ATX
326 UTC	327 ATX	328 ATX	329 TET	330 TET
331 ATX	332 ATX	333 MCI	334 ATX	335 SCH
336 ATX	337 FST	338 ATX	339 ---	340 ---
341 ATX	342 ATX	343 ATX	344 ATX	345 ATX
346 ATX	347 UTC	348 ATX	349 DCT	350 CSY
351 ATX	352 ATX	353 ---	354 ---	355 ---
356 ATX	357 ---	358 ATX	359 UTC	360 ---
361 CAN	362 ATX	363 CAN	364 HNI	365 MCI
366 UTC	367 ATX	368 ATX	369 TDD	370 TDD
371 ---	372 ATX	373 TDD	374 ---	375 TNO
376 ---	377 GTS	378 ---	379 ---	380 ---
381 ---	382 ATX	383 TDD	384 FDT	385 CAB
386 TBQ	387 CAN	388 ---	389 ---	390 ---
391 ---	392 ATX	393 EXF	394 ---	395 ---
396 ---	397 TDD	398 ---	399 ARZ	

421 ATX	422 ATX	423 ATX	424 ATX	425 TTH
426 ATX	427 ---	428 ATX	429 ---	430 ---
431 ATX	432 ATX	433 ATX	434 AGN	435 ATX
436 IDN	437 ATX	438 ATX	439 ---	440 TXN
441 ATX	442 ATX	443 ATX	444 MCI	445 ATX
446 ATX	447 ATX	448 ATX	449 ---	450 USL
451 ATX	452 ATX	453 ATX	454 ALN	455 ---
456 MCI	457 ATX	458 ATX	459 ---	460 ---
461 CAN	462 ATX	463 CAN	464 ---	465 CAN
466 ALN	467 ICT	468 ATX	469 ---	470 ---
471 ALN	472 ATX	473 ---	474 ---	475 TDD
476 TDD	477 ---	478 AAM	479 ---	480 ---
481 ---	482 ATX	483 ---	484 TDD	485 TDD
486 TDX	487 ---	488 ---	489 TOM	490 ---
491 ---	492 ATX	493 ---	494 ---	495 ---
496 ---	497 ---	498 ---	499 ---	

521 ATX	522 ATX	523 ATX	524 ATX	525 ATX
526 ATX	527 ATX	528 ATX	529 MIT	530 ---
531 ATX	532 ATX	533 ATX	534 ---	535 ATX
536 ALN	537 ATX	538 ATX	539 ---	540 ---
541 ATX	542 ATX	543 ATX	544 ATX	545 ATX

546 UTC	547 ATX	548 ATX	549 ---	550 CMA
551 ATX	552 ATX	553 ATX	554 ATX	555 ATX
556 ATX	557 ALN	558 ATX	559 ---	560 ---
561 CAN	562 ATX	563 CAN	564 ---	565 CAN
566 ALN	567 CAN	568 ---	569 ---	570 ---
571 ---	572 ATX	573 ---	574 AMM	575 ---
576 ---	577 GTS	578 ---	579 LNS	580 WES
581 ---	582 ATX	583 TDD	584 TDD	585 ---
586 ATC	587 LTQ	588 ATC	589 LGT	590 ---
591 ---	592 ATX	593 TDD	594 TDD	595 ---
596 ---	597 ---	598 ---	599 ---	

621 ATX	622 ATX	623 ---	624 ATX	625 NLD
626 ATX	627 MCI	628 ATX	629 ---	630 ---
631 ATX	632 ATX	633 ATX	634 ATX	635 ATX
636 CQU	637 ATX	638 ATX	639 BUR	640 ---
641 ATX	642 ATX	643 ATX	644 CMA	645 ATX
646 ---	647 ATX	648 ATX	649 ---	650 ---
651 ---	652 ATX	653 ---	654 ATX	655 ---
656 ---	657 TDD	658 TDD	659 ---	660 ---
661 CAN	662 ATX	663 CAN	664 UTC	665 CAN
666 MCI	667 CAN	668 CAN	669 UTC	670 ---
671 ---	672 ATX	673 TDD	674 TDD	675 ---
676 ---	677 ---	678 MCI	679 ---	680 ---
681 ---	682 ATX	683 MTD	684 ---	685 ---
686 LGT	687 NTS	688 ---	689 ---	690 ---
691 ---	692 ATX	693 ---	694 ---	695 ---
696 ---	697 ---	698 NYC	699 PLG	

720 TGN				
721 ---	722 ATX	723 ---	724 RTC	725 SAN
726 UTC	727 MCI	728 TDD	729 UTC	730 ---
731 ---	732 ATX	733 UTC	734 ---	735 UTC
736 UTC	737 MEC	738 MEC	739 ---	740 ---
741 MIC	742 ATX	743 EDS	744 ---	745 ---
746 ---	747 TDD	748 TDD	749 TDD	750 ---
751 ---	752 ATX	753 ---	754 TSH	755 ---
756 ---	757 TID	758 ---	759 MCI	760 ---
761 ---	762 ATX	763 ---	764 AAM	765 ---
766 ---	767 UTC	768 SNT	769 ---	770 GCN
771 SNT	772 ATX	773 CUX	774 ---	775 ---
776 UTC	777 MCI	778 UTC	779 TDD	780 TDD
781 ---	782 ATX	783 ALN	784 ALG	785 SNH
786 *1	787 ---	788 ---	789 TMU	790 ---
791 ---	792 ATX	793 ---	794 ---	795 ---
796 ---	797 TID	798 TDD	799 ---	

821 ATX	822 ATX	823 THA	824 ATX	825 MCI
826 ATX	827 UTC	828 ATX	829 UTC	830 ---
831 ATX	832 ATX	833 ATX	834 ---	835 ATX
836 TDD	837 TDD	838 ---	839 VST	840 ---
841 ATX	842 ATX	843 ATX	844 LDD	845 ATX
846 ---	847 ATX	848 ATX	849 ---	850 TKC
851 ATX	852 ATX	853 ---	854 ATX	855 ATX
856 ---	857 TLS	858 ATX	859 ---	860 ---
861 ---	862 ATX	863 ALN	864 TEN	865 ---
866 ---	867 ---	868 SNT	869 UTC	870 ---
871 ---	872 ATX	873 MCI	874 ATX	875 ALN
876 MCI	877 UTC	878 ALN	879 ---	880 NAS
881 NAS	882 ATX	883 ---	884 ---	885 ATX
886 ALN	887 ETS	888 MCI	889 ---	890 ---

891 ---	892 ATX	893 ---	894 ---	895 ---
896 TXN	897 ---	898 CGI	899 TDX	
921 ---	922 ATX	923 ALN	924 ---	925 ---
926 ---	927 ---	928 CIS	929 ---	930 ---
931 ---	932 ATX	933 ---	934 ---	935 ---
936 RBW	937 MCI	938 ---	939 ---	940 TSF
941 ---	942 ATX	943 ---	944 ---	945 ---
946 ---	947 ---	948 ---	949 ---	950 MCI
951 BML	952 ATX	953 ---	954 ---	955 MCI
956 ---	957 ---	958 *2	959 *2	960 CNO
961 ---	962 ATX	963 SOC	964 ---	965 ---
966 TDX	967 ---	968 TED	969 TDX	970 ---
971 ---	972 ATX	973 ---	974 ---	975 ---
976 ---	977 ---	978 ---	979 ---	980 ---
981 ---	982 ATX	983 WUT	984 ---	985 ---
986 WUT	987 ---	988 WUT	989 TDX	990 ---
991 ---	992 ATX	993 ---	994 ---	995 ---
996 VOA	997 ---	998 ---	999 MCI	

Notes
~~~~~
*1 -- Released For Future Assignment
*2 -- These NXX codes are generally reserved for test applications; They may be reserved for Access Tandem testing from an End Office.

Note also: The following NXXs are dedicated for RCCP (Radio Common Carrier Paging) under the discretion of the local exchange carrier:

202, 212, 302, 312, 402, 412, 502, 512, 602, 612, 702, 712, 802, 812, 902, and 912.

OCN Reference List
~~~~~~~~~~~~~~~~~~

ADG - Advantage Network, Inc.	AGN - AMRIGON
ALG - Allnet Communication Services	AMM - Access Long Distance
AAM - ALASCOM	ARE - American Express TRS
ARZ - AmeriCall Corporation (Calif.)	ATC - Action Telecom Co.
ATX - AT&T	BML - Phone America
BUR - Burlington Tel.	CAB - Hedges Communications
CAN - Telcom Canada	CNO - COMTEL of New Orleans
CQU - ConQuest Comm. Corp	CSY - COM Systems
CUX - Compu-Tel Inc.	CYT - ClayDesta Communications
DCT - Direct Communications, Inc.	DLT - Delta Communications, Inc.
EDS - Electronic Data Systems Corp.	ETS - Eastern Telephone Systems, Inc.
EXF - Execulines of Florida, Inc.	FDG - First Digital Network
FDN - Florida Digital Network	FDT - Friend Technologies
FST - First Data Resources	GCN - General Communications, Inc.
GTS - Telenet Comm. Corp.	HNI - Houston Network, Inc.
ITT - United States Transmission System	LDD - LDDS-II, Inc.
LDL - Long Distance for Less	LGT - LITEL
LNS - Lintel Systems	LSI - Long Distance Savers
LTQ - Long Distance for Less	MAL - MIDAMERICAN
MCI - MCI Telecommunications Corp.	MDE - Meade Associates
MEC - Mercury, Inc.	MIC - Microtel, Inc.
MIT - Midco Communications	MTD - Metromedia Long Distance
NLD - National Data Corp.	NTK - Network Telemanagement Svcs.
NTS - NTS Communications	ONC - OMNICALL, Inc.
ONE - One Call Communications, Inc.	PHE - Phone Mail, Inc.

PLG - Pilgrim Telephone Co.
PRO - PROTO-COL
RBW - R-Comm
RTC - RCI Corporation
SAN - Satelco
SCH - Schneider Communications
SDY - TELVUE Corp.
SIR - Southern Interexchange Services
SLS - Southland Systems, Inc.
SNH - Sunshine Telephone Co.
SNT - SouthernNet, Inc.
SOC - State of California
TBQ - Telecable Corp.
TDD - Teleconnect
TDX - Cable & Wireless Comm.
TED - TeleDial America
TEM - Telesystems, Inc.
TEN - Telesphere Network, Inc.
TET - Teltec Savings Communications Co
TGN - Telemanagement Consult't Corp.
THA - Touch America
TID - TMC South Central Indiana
TKC - TK Communications, Inc.
TLS - TELE-SAV
TMU - Tel-America, Inc.
TNO - ATC Cignal Communications
TOM - TMC of Montgomery
TOR - TMC of Orlando
TSF - SOUTH-TEL
TSH - Tel-Share
TTH - Tele Tech, Inc.
TTU - Total-Tel USA
TXN - Tex-Net
USL - U.S. Link Long Distance
UTC - U.S. Telcom, Inc. (U.S. Sprint)
VOA - Valu-Line
VST - STAR-LINE
WES - Westel
WUT - Western Union Telegraph Co.

NOTE: Where local telcos, such as Illinois Bell, offer 800 service, they purchase blocks of numbers from AT&T on prefixes assigned to AT&T. They are free to purchase blocks of numbers from any carrier of their choice however.

This list also applies to the 900/OCN Translation Table (presented later in this file).

900 Service
~~~~~~~~~~~

As I mentioned earlier there are two flavors of 900 service, AT&T and "everybody else." Everybody else is handled exactly as the 800 service above, except the IEC will probably use the ANI information to send you a bill (either directly, or through your BOC, each situation governed by applicable tariffs and contractual arrangements between the IEC and the BOC).

AT&T 900 is a curious monster indeed. It was designed as a "mass termination" service. When you dial a 900 by AT&T (such as the "hear space shuttle mission audio" number) you get routed to one of twelve "nodes" strewn throughout the country. These nodes are each capable of terminating 9,000 calls >PER SECOND<. There are several options available where the customer and/or the IP pay for all/part of the call. The big difference between 800 and AT&T 900 is >NOT< "who pays for the call" (there are free 900 numbers), but "how many people can it handle at once." The IP is responsible for providing program audio. AT&T is prohibited from providing audio-program services (i.e. tape recorded messages). As with any rule, there are exceptions to these as well.

I have included the entire 900-NXX to long-distance carrier translation table.
- -

Revised 900/OCN Translation Table
Effective October 10, 1988
~~~~~~~~~~~

Please note that this differs from the 800 table, because much fewer of the 900
NXXs are assigned.

NXX	OCN	NXX	OCN	NXX	OCN	NXX	OCN	NXX	OCN
200	ATX	202	Ameritech	210	ATX	220	ATX	221	TDX
222	ONC	223	TDX	225	Pac. Bell	226	MCI	233	TDX
234	TEN	240	U.S. West	248	Ameritech	250	ATX	258	TEN
254	TTU	255	SNT	260	ATX	264	ADG	266	CSY
272	Bell Atl.	273	CAN	275	ITT	280	Ameritech	282	LGT
283	Pac. Bell	288	GTE N.west	297	CAN	300	ATX	301	Ameritech
302	Ameritech	303	Pac. Bell	321	TEN	322	TDX	327	ETS
328	ATX	331	TET	332	PLG	333	U.S. West	335	Bell Atl.
342	ATX	344	ATX	345	ALN	346	United Tel.	350	ATX
364	GTE N.West	366	ONC	369	TEN	370	ATX	377	GTS
386	United Tel.	388	SNT	399	ARZ	400	ATX	407	ATX
410	ATX	420	ATX	422	ALN	426	PLG	428	Ameritech
430	U.S. West	444	ONC	445	PHE	446	MCI	450	Ameritech
451	CAN	456	TEN	463	United Tel.	478	AAM	479	ARZ
480	ATX	483	GTE Midwest	488	ONC	490	U.S. West	500	ATX
505	Pac. Bell	520	ATX	529	MIT	536	BUR	540	ALN
543	ALN	545	GTE Calif.	550	ALN	555	ATX	567	ALN
580	U.S. West	590	ATX	595	CAN	600	ATX	620	Ameritech
624	Pac. Bell	626	CSY	628	Ameritech	630	CAN	633	MIT
639	PLG	643	CAN	645	CAN	650	ATX	654	TEN
656	SNT	660	ATX	661	United Tel.	663	MDE	665	ALN
666	ONC	670	CAN	677	CAN	678	MCI	680	ATX
686	LTG	690	CAN	698	NY Tel.	699	PLG	701	Bell Atl.
710	TGN	720	ATX	722	Pac. Bell	724	RTC	725	SNT
727	GTE Calif.	730	ATX	739	CSY	740	ATX	741	TEN
746	ITT	750	CAN	753	ALN	765	ALN	773	ATX
777	Pac. Bell	778	Ameritech	780	Ameritech	786	ATX	790	CAN
792	CAN	801	Bell Atl.	820	ATX	830	CAN	843	Pac. Bell
844	Pac. Bell	847	United Tel.	850	ATX	860	ATX	866	AAM
870	CAN	872	TEN	887	ETS	888	CIS	900	TDX
901	Bell Atl.	903	ATX	909	ATX	924	Ameritech	932	ATX
948	ARZ	949	MIC	963	TEN	970	MIC	971	MIC
972	MIC	973	MIC	974	ALN	975	ALN	976	ATX
988	MCI	990	MCI	991	ALG	993	SNT	999	TEN

700 Service

The last SAC we'll deal with is 700. I've seen ads on late-night television for Group Access Bridging service (GAB) under 700 numbers, with an elephantine dialing sequence. The one that comes to mind is 10041-1-700-777-7777. If you were to dial 1-700-555-4141 you will hear a recording announcing your Equal-Access carrier. (Some carriers ignore the last four digits, and any 700-555 number will give the announcement).

This is signalled the same as 800 service, and may or may not be billed ENTIRELY at the discretion of the IEC. In New York, under PSC tariff, you can order 900 and/or 700 blocking as well as 976, 970, 550, and 540 blocking in various combinations.

What in ONE carrier might be a customer service hotline (Dial 1-700-I AM LOST) might for another be a revenue product. There is LITTLE standardization of 700
usage from IEC to IEC.

The one last dialing pattern that is worth mentioning is what's called, "cut through dialing." Try dialing 10220. If Western Union comes to your town, you'll get a FG-A style dial tone. Presumably if you had a Western Union "Calling Card" you could dial a call.

- -

Glossary

ANI - Automatic Number Identification. An MF sequence that identifies your line for toll billing information. Often confused with ANAC (Automatic Number Announcement Circuit) which reads your number back in a synthesized voice.

BOC - Bell Operating Company. An often misused term that in general usage means, "Your local exchange carrier." Since most of the telephones in the country are served by what used to be the Bell system, we tend to use the term. The proper term in this case, however IS "Exchange Carrier [EC]" They provide service within your LATA.

FG-A - Feature Group A. Line Side termination for Long Distance carriers. The old 555-1234 for Widget Telephone Company then dial an access code and the number style dialing is called FG-A.

FG-B - Feature Group B. Trunk Side termination for Long Distance carriers. (aka ENFIA B). 950 service. This is LATA wide service, and doesn't cost the customer message units. ANI is only provided when the trunks terminate in the End Office (as opposed to an access tandem).

FG-D - Feature Group D. Trunk Side termination. Provides 10xxx dialing, 1+ pre-subscription dialing, and Equal Access 800/900 service. Only available in electronic offices and some 5XB offices (through a beastie called an Adjunct Frame.)

GAB - Group Audio Bridging. Where several people call the same number, to talk to other people calling the same number. "Party" or "Chat" lines.

IEC - Inter-Exchange Carrier. Someone who actually carries calls from place to place. AT&T, Sprint, MCI are all IECs.

IP - Information Provider. Someone who sells a value-added service over the telephone. Where you pay for the INFORMATION you're receiving, as well as the cost of TRANSPORT of the call.

NXX - Notation convention for what used to be called a "prefix". N represents the digits 2 through 9, and X represents the digits 0 through 9. There are 800 valid NXX combinations, but some are reserved for local use. (411 for Directory, 611 for Repair Bureau, 911 for emergency, etc.)

ONI - Operator Number Identification. In areas with some styles of party-line service, the CO cannot tell who you are, and the operator will come on and say, "What number are you calling from?". You can lie, they have to trust you. They MAY know which PREFIX you're coming from, though.

PTN - Plant Test Number. A regular 10 digit number assigned with your inward

WATS line. This may NOT be a 'dialable' number from the local CO. (A friend has a WATS line in Amherst, MA [413-549,
dial the PTN locally, but you can if you come in on a toll trunk.)

SAC - Special Area Code. Bellcore speak for area codes that aren't really places, but classes of service.

==Phrack Inc.==

Volume Two, Issue 24, File 9 of 13

Lifting Ma Bell's Cloak Of Secrecy

A New Look At Basic Telephone Systems

by VaxCat

Though telephones predate radio communications by many years, they aren't nearly as simple as they appear at first glance. In fact, some aspects of telephone systems are most interesting and quite ingenious. In this file, I will describe some of these more interesting and perhaps less well-known areas of telephone systems. Before going any further, let me explain and apologize for the fact that some of the information in this file may not be altogether complete, up to date, or even totally correct.

I do not work for any phone company, and therefore, I do not have unlimited access to internal telephone company literature. Moreover, there is very little material available in books or magazines which describes how United States telephone systems work. Much of the information in this file has been obtained piece-meal from many different sources such as books, popular magazines, computer data communications journals, handbooks, and sometimes just
plain hearsay.

I have tried to correlate as much as possible all the little bits and pieces into a coherent picture which makes sense, but there is no easy way to be sure of all the little details. So think of this article as if it is a historical novel - generally accurate and, regardless of whether it is completely true or not, fascinating. With this out of the way, let's go on.

You, as a customer, are generally referred to as the "subscriber." Your telephone connects to the Central Office through a two-wire cable which may be miles long, and which may have a resistance on the order of hundreds or even thousands of Ohms. This cable is essentially a balanced line with a characteristic impedance of around 900 Ohms, but this varies greatly with different cables, different weather conditions, and different calls. This is why it is so hard to keep a hybrid phone-patch balanced.

The main power in the central office comes from 48 volt storage batteries which
are constantly kept trickle-charged. This battery is connected to your line through a subscriber relay and a balanced audio transformer. The relay is sensitive enough to detect even quite small currents through your line.

The buttons which stick up out of your telephone case when you lift the handset
activate the hook switch. The name probably dates back to the days when the handset (or even earlier, the earpiece) hung on the side of the phone from a hook. In any case, when your phone is hung up it is said to be on the hook, and when you lift the handset to make a call it is said to go off the hook. With the phone on hook, the line is connected only to the bell (called the ringer). Because the bell circuit has a capacitor in it, no DC current can flow through the phone. As a result, the subscriber relay back in the central

office will be de-energized, indicating to the central office (let's abbreviate
that as CO from now on) that your phone is hung up.

Since there is no current through your line or phone, there is no voltage drop anywhere, and so if you measure the voltage across the phone line at your phone
you will see the entire 48 volts (or even more if the CO batteries are well charged).

The positive (grounded) lead is called the tip and the negative lead is called the ring; these names correspond to the tip and ring of a three-circuit phone plug. Now suppose you want to place a call; You pick up the handset and the phone goes off the hook. This completes the DC circuit through the dial, microphone, and the hybrid network which is basically a complicated transformer
circuit.

At this point current starts to flow from the battery through your line and phone, and the subscriber relay back at the CO pulls in. The line voltage across your phone now drops to just a few volts because the line is loaded down
by the low resistance of the phone. The CO now searches for some idle dialing circuits, and when it finds them, connects a dial tone back to your phone. When you hear this, you start dialing.

So lets talk about rotary dial, the type of phone which you turn with your finger (we will talk about Touchtone dials later). When you dial a number, the
dial acts as a short circuit until you release the dial and let the built-in spring return it back to the resting position. As it is returning, it starts to open and close the circuit in sequence to indicate the number you dialed. If you dial a 1, it opens the circuit once; if you dial a 9 it opens the circuit nine times. As the dial is returning it cause the subscriber relay to open and close in step. This enables the CO to recognize the number you want. When you finish dialing, the dial becomes just a plain short circuit which passes current through the microphone and the hybrid network. Since the mike is a carbon unit, it needs this current to work. When the CO receives he complete number, it starts to process your call. If you dialed another subscriber in the same area, it may connect you directly to that subscriber's line. Calls to phones a little further away may have to be routed through another CO, while long distance calls may go through one or more long distance switching centers (called tandems) and possibly many other CO's before arriving
at the destination. At the completion of this process, you may get either a ringing signal, indicating that the phone at the other end is ringing, one of several types of busy signals, or possibly just silence, if something goes wrong somewhere.

When you talk to the person at the other end, the cable carries audio in both directions at the same time. Your carbon microphone varies the current in your
circuit, and this current variation is detected by a balanced transformer in the CO. At the same time, audio coming back to your phone goes through the hybrid network to your earphone. In phone company lingo they like to call the mike a transmitter, and the earphone is called the receiver.

You may be interested in the makeup of the various tones you may hear on your telephone; these tones are important to people such as computer communications designers who have to build equipment which will recognize dial or other signaling tones:

Dial tone in older exchanges may still be a combination of 120 and 600 Hz, but the newer exchanges use a combination of 350 and 440 Hz. There is often a slight change in the DC line voltage at the beginning of dial tone, and this may also be detected.

Busy signal is a combination of 480 and 620 Hz which alternates for 1/2 second on and 1/2 second off (i.e., 60 interruptions per minute) when the party you are calling is busy.

The same busy signal may be used for other conditions such as busy interoffice or long distance circuits, but would then be interrupted either 30 times a minute or 120 times per minute. This is a standard agreed on by an international telecommunications organization called CCITT (and I don't offhand remember the French words it stands for), but occasionally other frequencies up to 2 kHz are used. A siren-like sound varying between 200 and 400 Hz is often used for other error conditions.

The ringing tone, which you hear coming back to you when the phone rings on the other end of the connection, is nowadays mostly a combination of 440 and 480 Hz, but there is great variation between CO's. Very often a higher frequency such as 500 Hz is interrupted at 20 Hz, and other tones are used as well. The tone is usually on for 2 seconds and off for 4 seconds.

The ringing current, actually used to ring the bell in a telephone, is an AC voltage since it has to activate a ringer which has a capacitor in series with it. Different companies use different ringing currents, but the most common is 90 volts at 20 Hz. Since a typical phone may be thousands of feet away from the CO, the thin wires used may have a fairly high line resistance. Hence only a relatively small current can be applied to the bell, certainly not enough to ring something like a doorbell. This problem is solved by making the bell resonant mechanically at the ringing frequency so that even a fairly small amount of power is enough to start the striker moving hard enough to produce a loud sound. This is the reason why a low-frequency AC is used. Although this raises some problems in generating a 20 Hz signal at a high enough voltage, it has the advantage that a bell will respond to a ringing current only if the frequency is quite close to the bell's naturally resonant frequency. If you build two bells, one resonant at 20 Hz and the other resonant at 30 Hz, and connect them together to the same line, you can ring just one bell at a time by connecting a ringing current of the right frequency to the line; this has some useful applications in ringing just one phone on a party line.

Now let's look at some of the components of the phone itself. We will consider the most common new phone, a model 500 C/D manufactured by Western Electric and used by Bell System affiliated phone companies. This is the standard desk phone, having modern rounded lines and usually having a G1 or G3 handset. It was developed about 1950 and replaced the older 300-series phones which had the older F1 handset and had sharper corners and edges. There was an in between phone, where they took an old 300-series phone and put a new case on it which resembled the 500-style case, but had a straight up and down back - the back of

the case came straight down right behind the handset cradle, whereas the true 500-style telephone has what looks like a set sticking out behind the cradle).

If you are still in doubt as to which phone you have, the bell loudness control
is a wheel on the 500-type phone and a lever on the 300-type. If you live in the boondocks, you may still have the 200-type phone (sometimes called the ovalbase) or maybe even the desk-stand type that looked like a candlestick, with the microphone mounted on the top and the earpiece hanging on the side from a hook.

Neither of these phones had a built in bell, and so you probably have a bell box attached to your wall. If you have a phone with a handle on the side which
you crack to call the operator, the following does not apply to your phone!

Now lets discuss the bell circuit, which consists of a two-coil ringer and a 0.5 uF capacitor. On Western Electric phones the capacitor is mounted inside the network assembly, which also has a large number of screws on top which act as connection points for almost everything inside the phone. I have never been able to find out why the ringer has two coils of unequal resistance, but it apparently has something to do with determining which subscriber on a party line makes which call. In most phones, the yellow and the green wires are connected together at the wall terminal block so that the bell is connected directly across the telephone line; disconnecting the yellow lead would turn off the bell (although sometimes the connection is made internally by connecting the black lead from the ringer directly to the L1 terminal, in which
case the yellow lead is disconnected.

You may wonder why a yellow lead is needed at all when only two wires are normally used anyway. It is true that only two wires enter the house from the outside; one of these is the tip and the other is the ring. In a non-party line the ringing current as well as all talk voltages are applied between the tip and the ring, and it doesn't actually matter which of the phone leads goes to the tip and which to the ring if you have a rotary dial phone. If you have a Touchtone dial, then you have to observe polarity so that the transistor circuit in the dial works, in which case you have to make sure that the green lead goes to the tip and the red lead goes to the ring.

The yellow lead is commonly used for party lines. On a two-party line ringing current from the CO is applied not between the two lines, but between one line and ground. In that case the yellow lead goes to ground while the other side of the ringer (the red lead) is connected to either the tip or the ring, depending on the party. In this way, it is possible to ring only one party's bell at a time.

The remaining connections inside the telephone are varistors; the phone companies must be the world's biggest users of these devices, which are variable resistors whose resistance drops as the voltage across them rises. Their function in the phone set is to short out parts of the set if the applied
voltage gets too high.

The hook switch actually has three sets of contacts, two normally open (open, that is, when the hand set is on hook) which completes the DC circuit when you pick up the handset, and a normally closed contact which is wired directly across the earphone. This contact's function is to short the earphone during the time that the DC circuit is being opened or closed through the phone - this
prevents you from being blasted by a loud click in the earphone.

The dial has two contacts. One of these is the pulsing contact, which is normally closed and only opens during dialing on the return path of the dial after you let go of it. The second contact (the off-normal contact), shorts the earphone as soon as you start turning the dial, and releases the short only after the dial returns back to the normal position. In this way you do not hear the clicking of the dial in the phone as you dial. Finally, the phone has the hybrid network which consists of a four-winding transformer and whole collection of resistors, capacitors, and varistors. The main function of the network is to attenuate your own voice to lower its volume in your earphone.

The simplest phone you could build would be just a series circuit consisting of a dial, a mike, and an earphone. But the signals coming back from the other party so much weaker than your own signals, that than earphone sensitive enough to reproduce clearly and loudly the voice of the other person would then blast your eardrums with the sound of your own voice. The function of the network is to partially cancel out the signal produced by the local mike, while permitting all of the received signal to go to the earphone. This technique is similar to the use of the hybrid phone patch with a VOX circuit, where you want the voice of the party on the telephone to go to your transmitter, but want to keep the receiver signal out the transmitter.

In addition to the parts needed for the hybrid, the network also contains a few other components (such as the RC network across the dial pulsing contacts) and screwtype connection points for the entire phone.

A Touchtone phone is similar to the dial phone described above, except that the rotary dial is replaced by a Touchtone dial. In addition to its transistorized tone generator, the standard Touchtone pad has the same switch contacts to mute the earphone, except that instead of completely shorting the earphone, as the rotary dial does, the Touchtone dial switches in a resistor which only partially mutes the phone.

It is fairly common knowledge as to what frequencies are used for Touchtone signalling, but a it never hurts to reiterate information. Each digit is composed of one frequency from the low group and one frequency from the high group; for instance, the digit 6 is generated by producing a low tone of 770 Hz (Hertz) and a high tone of 1477 Hz at the same time. The American Touchtone pads generate both of these tones with the same transistor, while European pads (yes, there are some) use two transistors, one for reach tone. In addition to the first three high tones, a fourth tone of 1633 Hz has been decided on for generating four more combinations. These are not presently in use, although the standard phone Touchtone pad can easily be modified to produce this tone, since the required tap on the inductor used to generate the the tone is already present and only an additional switch contact is needed to use it.

What is not generally known is that the United States Air Force uses a

different set of Touchtone frequencies, in the range of 1020 to 1980 Hz. Since
many of the phones available for purchase in stores come from Department of Defense surplus sales, it will be interesting when these phones become available.

Another Touchtone dial presently used by amateurs is made up from a thin elastomeric switch pad made by the Chomerics Corporation (77 Dragon Court, Woburn, Mass. 01801) and a thick-film hybrid IC made by Microsystems International (800 Dorchester Boulevard, Montreal, Quebec). The pad is the Chomerics ER-20071, which measures about 2 1/4 inch wide by 3 inches high, and only about 3/16 inch thick (Chomerics also makes a smaller model ER21289, but it is very difficult to use and also apparently unreliable). Microsystems International makes several very similar ICs in the ME8900 series, which use different amounts of power and generate different amounts of audio. Some of these also contain protection diodes to avoid problems if you use the wrong polarity on the IC, and there are so many models to choose from that you should
get the technical data from the manufacturer before ordering one. There are a number of United States distributors, including Newark Electronics, Milgray and
Arrow Electronics in New York.

One of the problems with any current IC oscillator is that the frequency changes if rf gets near it. Many hams are having a hard time mounting such IC pads on their 2 meter handie-Talkies. A solution seems in sight as Mostek, a large IC company, is coming out with an IC Touchtone generator which has a cheap 3.58 MHz external crystal as reference, and then produces the tone frequencies by dividing the 3.58 MHz down with flip flops to get the required tone frequencies. This approach not only promises to be more reliable in the presence of rf, but should also be cheaper since it would not need the custom (and expensive) laser trimming of components that the Microsystems International IC needs to adjust the frequencies within tolerance.

At the other end of the telephone circuit, in the CO, various circuits are used
to decode the digit you dial into the appropriate signals needed to perform the
actual connection. In dial systems, this decoding is done by relay circuits, such as steppers. This circuitry is designed for dialing at the rate of 10 pulses per second, with a duty cycle of about 60% open, 40% closed. The minimum time between digits is about 600 milliseconds, although a slightly greater time between digits is safer since it avoids errors.

In practice, many COs will accept dialing at substantially slower or faster rates, and often you will see a dial that has been speeded up by changing the mechanical governor to operate almost twice as fast; it depends on the type of CO equipment.

Touchtone decoding is usually done by filter circuits which separate out the Touchtone tones by filters and then use a transistor circuit to operate a relay. A common decoder is the 247B, which is designed for use in small dial switchboard systems of the type that would be installed on the premises of a business for local communication between extensions. It consists of a limiter amplifier, seven filters and relay drivers (one for each of the seven tones commonly used) and some timing and checking circuitry. Each of the seven relays has multiple contacts, which are then connected in various series/parallel combinations to provide a grounding of one of ten output contacts, when a digit is received. The standard 247B does not recognize the *
and digits, but can be modified easily enough if you have the unit diagram.

The 247B decoder is not very selective, and can easily be triggered by voice unless some additional timing circuits are connected at the output to require that the relay closure exceed some minimum time interval before it is accepted.
Slightly more complicated decoders which have the time delays built in are the A3-type and the C-type Touchtone Receivers. both of these are used in customer-owned automatic switchboards when a caller from the outside (via the telephone company) wants to be able to dial directly into the private switchboard to call a specific extension.

The C-type unit is similar to the 247B in that it has ten outputs one for each digit. The A3-type does not have output relays, but instead has seven voltage outputs, one for each of the seven basic tones, for activating external 48-volt
relays. The A-3 unit is ideal for activating a Touchtone encoder, which can then be used to regenerate the Touchtone digits if the original input is noisy.
This might be very useful in a repeater autopatch, for cleaning up Touchtone digits before they are sent into the telephone system.

In addition to the above, there are probably other types of units specially designed for use in the CO, but information on these is not readily available. It is also fairly easy to build a Touchtone decoder from scratch. Though the standard telephone company decoders all use filter circuits, it is much easier (though perhaps not as reliable) to use NE567 phase-locked-loop integrated circuits.

An interesting sidelight to Touchtone operation is that it greatly speeds up the process of placing a call. With a Touchtone dial it is possible to dial a call perhaps 3 or 5 times faster than with a rotary dial. Since the CO equipment which receives and decodes the number is only needed on your line during the dialing time, this means that this equipment can be switched off your line sooner and can therefore handle more calls. In fact, the entire Touchtone system was invented so that CO operation would be streamlined and less equipment would be needed for handling calls. It is ironic that the customer should be charged extra for a service which not only costs the telephone company nothing, but even saves it money.

Another practice which may or may not cost the company money is the connection of privately-owned extension phones. You have probably seen these sold by mail
order houses and local stores. The telephone companies claim that connecting these phones to their lines robs them of revenue and also may cause damage to their equipment. There are others, of course, who hold the opinion that the easy availability of extensions only causes people to make more calls since they are more convenient, and that the companies really benefit from such use. The question of damage to equipment is also not easily answered, since most of the extension phones are directly compatible, and in many cases the same type as the telephone company itself uses. Be that as it may, this may be a good time to discuss such use.

Prior to an FCC decision to telephone company interconnection in the Carterfone
case in 1968, all telephone companies claimed that the connection of any equipment to their lines was illegal. This was a slight misstatement as no specific laws against such use were on the books. Instead, each local telephone company had to file a tariff with the public service commission in that state, and one of the provisions of that tariff was that no connection of any external equipment was allowed. By its approval of that tariff, the public

service commission gave a sort of implicit legal status to the prohibition.

In the Carterfone case, however, the FCC ruled that the connection of outside equipment had to be allowed. The phone companies then relaxed their tariff wording such that connection of outside equipment was allowed if this connection was through a connecting arrangement provided by the telephone company for the purpose of protecting its equipment from damage. Although this
result has been challenged in several states, that seems to be the present status. The strange thing is that some telephone companies allow interconnection of customer equipment without any hassle whatsoever, while others really make things difficult for the customer.

==Phrack Inc.==

Volume Two, Issue 24, File 10 of 13

```
()()()()()()()()()()()()()()()()()()()
()                                  ()
()        Network Progression       ()
()                                  ()
()         by Dedicated Link        ()
()                                  ()
()           January 1989           ()
()                                  ()
()()()()()()()()()()()()()()()()()()()
```

This file provides a general overview of how networks have progressed from phone lines to T1 lines.

There are numerous reasons to share networking facilities. The concept of networking is to optimize all the aspects of voice and data transmission, and to utilize all the amounts of space in the transmission lines.

Not long ago companies used AT&T's switching facilities for all local calls. This means use of the Centrex, which is the switching of local calls by AT&T (which is much more expensive than using your own switching facilities). Then the larger organizations started to put in PBXes (Private Branch Exchange) to enable them to switch local calls (class 5 ESS) without having anything to do with AT&T. The process of using a PBX (or a Computerized Branch Exchange CBX) is much more efficient if the phone traffic is high. This is the beginning of a Local Area Network (LAN). Once an organization has it's own LAN it can lease the extra transmission space to another company, because they are paying for it anyway. Another method of bypassing AT&T's service is to use a foreign exchange (FX) line. Which is a long distance dedicated point-to-point private line, which is paid for on a flat rate basis. A FX line can be purchased from AT&T or many other vendors. These private lines (PL) are used with voice and data transmissions. Data transmission must have a higher grade quality than voice because any minor break in the transmission can cause major, expensive errors in data information being processed.

One of the most optimum ways of transmitting data is a T1 line which transmits data at 1.544 megabits per second. Microwave, Satellite, and Fiber Optic systems are being used for data transmission. These methods multiplex several lines into one to create greater capacity of the transmission. A multiplexed line has 24 channels that can be divided into the appropriate space needed to utilize each transmission (i.e. a simple voice transmission which has about 300-3000 Hz uses a small portion of the multiplexed line). There are two types of multiplexing; time-division and frequency. Time-division multiplexing divides the channels into separate time slots. Frequency-division multiplexing separates the different channels with the use of different bandwidths. Typically, data is transmitted through digital systems rather than analog. However, all the state-of-the-art equipment is now digital.

When the data is being processed from the computer to another computer there must be a standard protocol for communicating the interexchange within the network. The protocol is the set of rules that the computer says are necessary to have in order for the other computer to connect to it. This is the standard

way of communicating (The American Standard Code for Interface Interexchange, ASCII). Also, there are encryption codes which are used for security reasons. Encryption codes can be scrambled on a hourly, daily, weekly, or monthly basis,
depending on the level of security.

The information that is being sent is organized by packet switching. The most used packet switching is called X.25, and this is the interface that the CCITT (Comittee Consultif Interaction Telephonique & Telegraphique) recommends to use
for connection between the Data Terminal Equipment (DTE) and the Data Circuit-terminating Equipment (DCE).

Within this network it is crucial that there is software providing Automatic Route Selection (ARS). There must be an ARS (the least cost path length) programmed within the transmission. It is the job of the system analyst or operator to assign the proper cost of each path where the transmission goes in order for the packet to go through it's least cost route (LCR).

The packet travels through a path from it's source to it's final destination. The system analyst or operator must have full knowledge of the exact path length, the exact alternative path length, plus the exact third alternative path length. The path length is measured in hops, which equals to the number of circuits between central nodes. The system manager must set a maximum value
of hops at which the path can never exceed. This is the actual circuit cost which is assigned to each possible path. It is important that the system manager has knowledge of the circuit costs in order for the ARS to be programmed effectively.

These are just some of the basics that are involved in transmitting information
over a network. I hope it helped you lots!

_

==Phrack Inc.==

Volume Two, Issue 24, File 11 of 13

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                 PWN
PWN        P h r a c k   W o r l d   N e w s        PWN
PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~        PWN
PWN                Issue XXIV/Part 1                PWN
PWN                                                 PWN
PWN                February 25, 1989                PWN
PWN                                                 PWN
PWN          Created, Written, and Edited           PWN
PWN               by Knight Lightning               PWN
PWN                                                 PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Time And Time Again
~~~~~~~~~~~~~~~~~~~
Greetings to everyone! This issue of Phrack Inc. marks the completion of the plan I had conceived a little more than one year ago -- "The Phoenix Project." No, not the bulletin board run by The Mentor (although the name of the board came from this plan), my scheme to rebuild the hacking community from its remaining ashes of the "Crisis of 1987." My plan had several parts that needed to come together.

- Announce the plan and pour lots of hype into it to spur great enthusiasm.
- Hold SummerCon '88 in St. Louis, Missouri to get today's hackers to meet.
- Regain control of Phrack Inc. and put it back on its feet.
- Release the Vicious Circle Trilogy to expose and defeat our security problems.
- Bring today's hackers into the next Millennium with The Future Transcendent Saga (which helps to unite yesterday's hackers with the present).

And now...

Announcing The 3rd Annual...

SummerCon '89
~~~~~~~~~~~~~
Saint Louis, Missouri
July 23-25, 1989

The date is a tentative one, but I would imagine that it will not change.
For more information please contact Taran King or Knight Lightning.
- -
On the lighter side, this issue of Phrack World News contains articles dealing with Shadow Hawk, The Disk Jockey, Compaq, the FBI "Super" Database, the Australian-American Hackers Ring, Computer Emergency Response Team, StarLink, The Xenix Project, The Lost City of Atlantis, The Beehive BBS, and much more. So read it and enjoy.

For any questions, comments, submissions of articles, or whatever, I can be reached at C483307@UMCVMB.MISSOURI.EDU or C483307@UMCVMB.BITNET or whatever bulletin board you can find me on.

:Knight Lightning

Explosives Expertise Found In Computer January 5, 1989

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

by Matt Neufeld (The Washington Times)

One of the four Bethesda youths killed in an explosion in the garage at the home of the Brazilian Embassy's attache last weekend had access to a local computer system's how-to listing of bombs and explosives, according to a system member.

"He was highly involved with computers," said the computer operator of the 18-year-old Dov Fischman, one of the teens killed by the explosion. "Dov used to go over to my friend's house," where they discussed various types of software and computer systems, he said.

Located within an elaborate computer system of about 200 private bulletin boards is a board titled "The Lost City of Atlantis" that contains files under the following names: "Pipe Bombs," Gas Tank Bombs," "Make Smoke Bombs," "Soda Bombs," "Explosive Info," "Kitchen Improvised Plastic Explosives," and "Plastic Explosives," according to system files reviewed yesterday by the Washington Times.

Details on committing mischief and various illegal activities fill the files of Atlantis and other boards in the system. The Atlantis board is listed under the heading, "The Rules of Anarchy."

The files on Atlantis, which is run locally, but could be accessed by computer owners nationwide, include information and correspondence on how to buy various chemicals and and explosives used to make bombs. Other files have explanations on how to use these materials to fashion the bombs.

"Some or all of you reading this may have caught word from the grapevine that I sell laboratory materials and/or chemicals," begins one message from a system worker who operates under the pseudonym "The Pyromaniac."

"I can get for you almost any substance you would want or need," the message says later. "Always remember that I am flexible; Your parents need not know about the chemicals."

Mr. Fischman and the other teens have been described by friends and relatives as highly intelligent, hard-working honor students. They were killed about 3:15 a.m. Saturday in an explosion at the home of attache Vera Machado in the 6200 block of Verne Street. A Montgomery County Police investigation determined the cause was accidental and caused by the youths "experimenting with some type of explosive."

Nitrates, peroxides and carbonates were found at Mr. Fischman's home, along with literature on "resources for chemicals and appliances and recipes utilized for explosive devices," said fire marshal's spokesman Mike Hall. "The exact nature of resources and recipes has not been disclosed by the investigative section, as the investigation is going on."
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

"I have no knowledge that any computer system information was used," but that possibility will be investigated, Mr. Hall said. Mr. Fischman's father, Joel, yesterday said his son and the other three youths were involved with computers.
But he said he was not aware of any connection between computers and the explosion. He referred further questions to the police.

The local computer system operator said most users are 15 to 19 years old. The
operator, however, said it is common for users of the system to peruse the files while their parents have no knowledge of the contents.

The boards and files are legal, and the bomb information is primarily confined to "private" bulletin boards created by persons known as "system operators."

However, anyone with a home computer, a telephone and a modem can hook up to the bulletin boards if they gain approval of the individual operators, the operator said.

"I think this should be allowed, but not just for any kids," said the operator,
who is an adult. He said it's "really the parents' fault" for not supervising their children's computer access.

Another board in the system, "Warp Speed," also provides information on explosives. That board was shut down sometime between December 30, 1988 and January 1, 1989 the operator said. That board is "host" to "Damage, Inc.," which is a "group of people who concentrate on explosives, things to screw people up, damage," he said.

In the "Beehive" board the following message appears from "Mister Fusion:"

> "low cost explosives are no problem. make them yourself. what do you want rdx? detonators, low explosives? high explosives? i can tell you what to do for some, but I would reccomend (sic) cia black books 1-3."

Other boards and files in the system include information on computer hacking, constructing a device to jam police radar detectors, picking locks, and "phreaking," which is computer jargon for using computers to make free telephone calls.

Some of these files are: "Making LSD," "Listing of common household chemicals,"
"Info on Barbiturates," "Make a mini-flame thrower," How to make a land mine," "How to Hot Wire a car," "Home Defense: part II, guns or friends," "How to have
fun with someone else's car," "Fun! with Random Senseless Violence," "Picking up little girls," and "How to break into a house."

"A lot of the information is wrong, in the phreaker world, regarding ways to defeat the telephone company," said the operator, who has been involved with computers for at least six years. "But the bomb information is pretty much accurate."

In the two page, "High Explosives" file, there are detailed explanations on how
to use the chemicals cacodyal, tetryl and mercury fulminate.

"This stuff is awesome," begins the section on cacodyal. "It is possesses

flammability when exposed to air. Plus it will release a cloud of thick white smoke. The smoke just happens to be arsenic."

The file does offer this warning at the end: "Don't attempt to make these things unless you are experienced in handling chemicals. They can be very dangerous if not handled properly."

The "Kitchen Improvised Plastic Explosives" file, which instructs users on "how
to make plastique from bleach" and is credited to a Tim Lewis, warns that the chemicals are dangerous."

Computer Emergency Response Team (CERT) January 23, 1989

~~~~~~

Excerpted from UNIX Today

WASHINGTON -- The federal government's newly formed Computer Emergency Response
Team (CERT) is hoping to sign up 100 technical experts to aid in its battle against computer viruses.

CERT, formed last month by the Department of Defense's Advanced Research Project Agency (DARPA), expects to sign volunteers from federal, military, and civilian agencies to act as advisors to users facing possible network invasion.

DARPA hopes to sign people from the National Institute of Science and Technology, the National Security Agency, the Software Engineering Institute, and other government-funded university laboratories, and even the FBI.

The standing team of UNIX security experts will replace an ad hoc group pulled together by the Pentagon last November to deal with the infection of UNIX systems allegedly brought on by Robert Morris Jr., a government spokesman said.

CERT's charter will also include an outreach program to help educate users about what they can do the prevent security lapses, according to Susan Duncal, a spokeswoman for CERT. The group is expected to produce a "security audit" checklist to which users can refer when assessing their network vulnerability. The group is also expected to focus on repairing security lapses that exist in current UNIX software.

To contact CERT, call the Software Engineering Institute at Carnegie-Mellon University in Pittsburgh at (412) 268-7090; or use the Arpanet mailbox address cert@sei.cmu.edu.

The Xenix Project aka The Phoenix Project Phase II January 1989

~~~~~~

There are some big changes in store for everyone's favorite bulletin board.

As of January 25, 1989, The Mentor became the proud owner of the complete SCO Xenix system, complete with the development kit and text utilities (a $1200 investment, but worth it). He has arranged for a UUCP mail and USENET newsfeed, and is working on getting bulletin board software up and running on it.

So what does this mean to you? As I have been illustrating throughout The Future Transcendent Saga and a few other files/places, the future lies in the wide area networks. So now for the first time ever, The Mentor is offering the
hackers a cheap, *LEGAL* way to access the gigabytes of information available through USENET. Mail can be sent through BITNET, MILNET, ARPANET, and INTERNET
gateways to users all over the world. In short, connectivity has arrived and the future grows ever closer.

The first thing that The Mentor wants to do is get a second hard disk drive. There is no way the Xenix Project can run right now without it. His 40 meg has
a 20 meg Xenix partition, 17 megs of which is occupied by the /root/ file system. The MS-DOS partition has 12 megs of the board, plus all the programs he needs to exist (Pagemaker, Word, Microsoft C, Brief, etc). A *MINIMUM* of a
60 meg drive will be needed to support the newsfeed (USENET generated 50 megs of traffic in the last 2 weeks). A 100+ meg drive would be better. Once a hard disk is obtained, the system will go online as a single-line UNIX machine.
Hopefully, enough money will be generated to add a second phone line and modem quickly. At this point the system will begin to take off.

The Mentor's eventual goal (inside 6 months) is to have 4-6 300-2400 baud lines
available for dialin on a hunt group, plus a 19.2Kbaud line for getting the USENET feed. The estimated startup cost for a 5-line system is:

110 meg hard disk.....	$1000
4 2400 baud modems (I've got 1 already)..	$ 525
Installation of 4 phone lines.....	$ 450
MultiPort Serial Card.....	$ 300
SCO Xenix Software.....	$1200
	~~
	$3475

Financing is a problem. The Mentor has already sunk the $1200 into the Xenix package (plus his original purchase of the computer system), leaving him $2200 away from the best hacker system in the world. There are two ways that he hopes on getting the money for the rest of the system.

A) Donations - Many users have already indicated that they will send in anywhere from $10 to $100. Surprisingly enough, the security people on The Phoenix Project have been extremely generous. There *is* an incentive to donate, as will be shown below.
B) Monthly fees - There will be a $5-$12.50 charge per month to use the UNIX side of the system, but the Phoenix Project BBS will remain free! Here is how it works:

Level 1 - BBS Only. Anyone who wishes to use only The Phoenix Project will call and log in to account name 'bbs.' They will be forced into the BBS software, at which point they will log in as usual. As far as they're concerned, this is just a change of software with the addition of the front end password 'bbs.'

Level 2 - Individual Mail & News account. For $5 a month, a user will get their own private account with full access to UUCP mail and USENET news. They will be able to send mail all over the world and to read and post to the hundreds of USENET newsgroups. Legally, for a change!

Level 3 - Individual Mail, News, Games, and Chat. The user will have all the privileges of a Level 2 person, be able to access games such as Rogue, Chase, and Greed, plus will have access to the multi-user chat system similar to the one running on Altos in West Germany, allowing real-time conferencing between hackers here in the states without having to have an NUI to get to Datex-P. This will cost $10 per month.

Level 4 - Full Bourne Shell access. This will allow access to the full system, including the C compiler, text utilities, and will include access to
the online laser printer for printing term papers, important documents, or anything else (mailing will incur a small fee.) Level 4 access will be restricted to people technically sophisticated enough to know how to use and
how not to use UNIX compilers. The entire Xenix Development System and Text Processing Utilities are installed, including online manual pages. I will aid people in debugging and testing code whenever needed. Charge is $12.50 per month.

C) Why Donate? - Simple. You get a price break. Here are the charter membership categories:

Contributing: $20 You receive 6 months of Level 2 access, a $10 savings over the monthly fees.

Supporting: $45 You receive either 1 year of Level 2 access or 6 months of Level 3 access.

Sustaining: $75 You receive 1 year of Level 3 access, or life time level 2 access.

Lifetime: $100 You receive lifetime Level 4 access. Contributions in amounts less than $20 will be directly applied toward Level 2 access (e.g. A $10 donation will give you 2 months Level 2 access).

Hardware contributions will definitely be accepted in return for access.
Contact me and we'll cut a deal.

Information Provided by The Mentor

- -

A Few Notes From The Mentor
~~~~~~~~~~~~~~~~~~~~~~~~~~~

People -- I am not trying to make a profit off of this. If I could afford the hardware I'd buy it. The Phoenix Project has been committed to bringing you the best in hack/phreak information available, and will continue to do so FREE.

I stress, even after the switch is made, The Phoenix Project BBS will be available under a un-pass-worded login that anyone can log into and use. It's only if you want to enter the world of networks in a *LEGAL* manner that I need
to get money .

The system will expand as interest in it expands. If I never get enough paid users to add more than one line, it will remain a one-line system. I think enough people will see the advantages of UUCP and USENET to be willing to shell
out the cost of a 6-pack of good beer to get access.
~~~~~~~~~~~~~~~~~~~~~~~~~~~

As a side note to UNIX hacks out there, this system will also offer a good place to explore your UNIX hacking techniques. Unlike other systems that penalize you for breaking security, I will reward people who find holes in my security. While this will mostly only apply to Level 4 people (the only ones not in a restricted shell), 3-6 months of free access will be given to people discovering security loopholes. So if you've ever wanted an unrestricted environment for learning/perfecting your UNIX, this is it!

For more information, I can be reached at:

The Phoenix Project: 512-441-3088
Shadowkeep II: 512-929-7002
Hacker's Den 88: 718-358-9209

Donations can be sent to: Loyd
PO Box 8500-615
San Marcos, TX 78666
(make all checks payable to Loyd)

+++The Mentor+++

"The Future is Forever!"

Breaking Into Computers Is A Crime, Pure And Simple December 4, 1988
~~~~~~

By Edward A Parrish Jr., Past President, IEEE Computer Society
Originally printed in Los Angeles Times

During the last few years, much has been written to publicize the feats of computer hackers. There was, for example, the popular movie War Games, about a teen-ager who, using his home computer, was able to tap into a military computer network and play games with the heart of the system. The games got of control when he chose to play "thermonuclear war." The teen-ager, who was depicted with innocent motives, eventually played a crucial role in solving the problem and averting a real nuclear exchange, in the process emerging as hero.

A real-life example in early November involved a so-called computer virus (a self-replicating program spread over computer networks and other media as a prank or act of vandalism), which nearly paralyzed 6,000 military and academic computers.

Unfortunately, perhaps because the effect of such "pranks" seems remote to most people, it is tempting to view the hacker as something of a folk hero - a lone individual who, armed with only his own ingenuity, is able to thwart the system. Not enough attention is paid to the real damage that such people can do. But consider the consequences of a similar "prank" perpetrated on our air-traffic control system, or a regional banking system, or a hospital information system. The incident in which an electronic intruder broke into an unclassified Pentagon computer network, altering or destroying some files, caused potentially serious damage.

We do not really know the full effect of the November virus incident that
~~~~~~

brought many computers on the Cornell-Stanford network to a halt, but credible published estimates of the cost in man-hours and computer time have been in the millions of dollars. The vast majority of professional computer scientists and engineers who design, develop, and use these sophisticated networks are dismayed by this total disregard of ethical practice and forfeiture of professional integrity.

Ironically, these hackers are perhaps driven by the same need to explore, to test technical limits that motivates computer professionals; they decompose problems, develop an understanding of them and then overcome them. But apparently not all hackers recognize the difference between penetrating the technical secrets of their own computer and penetrating a network of computers that belong to others. And therein lies a key distinction between a computer professional and someone who knows a lot about computers.

Clearly a technical degree is no guarantee of ethical behavior. And hackers are not the only ones who abuse the power inherent in their knowledge. What, then, can we do?

For one thing, we - the public at large - can raise our own consciousness; Specifically, when someone tampers with someone else's data or programs, however clever the method, we all need to recognize that such an act is at best irresponsible and very likely criminal. That the offender feels no remorse, or that the virus had unintended consequences, does not change the essential lawlessness of the act, which is in effect breaking-and-entering. And asserting that the act had a salutary outcome, since it lead to stronger safeguards, has no more validity than if the same argument were advanced in defense of any crime. If after experiencing a burglary I purchase a burglar alarm for my house, does that excuse the burglar? Of course not. Any such act should be vigorously prosecuted.

On another front, professional societies such as the IEEE Computer Society can take such steps to expel, suspend, or censure as appropriate any member found guilty of such conduct. Finally, accrediting agencies, such as the Computing Sciences Accreditation Board and the Accreditation Board for Engineering and Technology, should more vigorously pursue their standards, which provide for appropriate coverage of ethical and professional conduct in university computer science and computer engineering curriculums.

We are well into the information age, a time when the computer is at least as vital to our national health, safety and survival as any other single resource.
The public must insist on measures for ensuring computer security to the same degree as other technologies that are critical to its health and safety.

—

==Phrack Inc.==

Volume Two, Issue 24, File 12 of 13

PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN PWN
PWN P h r a c k W o r l d N e w s PWN
PWN ~~~~~~~~~~ ~~~~~~~~~ ~~~~~~~ PWN
PWN Issue XXIV/Part 2 PWN
PWN PWN
PWN February 25, 1989 PWN
PWN PWN
PWN Created, Written, and Edited PWN
PWN by Knight Lightning PWN
PWN PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN

Shadow Hawk Gets Prison Term February 17, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~

An 18 year old telephone phreak from the northside/Rogers Park community in Chicago who electronically broke into U.S. military computers and AT&T computers, stealing 55 programs was sentenced to nine months in prison on Tuesday, February 14, 1989 in Federal District Court in Chicago.

Herbert Zinn, Jr., who lives with his parents on North Artesian Avenue in Chicago was found guilty of violating the Computer Fraud and Abuse Act of 1986 by Judge Paul E. Plunkett. In addition to a prison term, Zinn must pay a $10,000 fine, and serve two and a half years of federal probation when released from prison.

United States Attorney Anton R. Valukas said, "The Zinn case will serve to demonstrate the direction we are going to go with these cases in the future. Our intention is to prosecute aggressively. What we undertook is to address the problem of unauthorized computer intrusion, an all-too-common problem that is difficult to uncover and difficult to prosecute..."

Zinn, a dropout from Mather High School in Chicago was 16-17 years old at the time he committed the intrusions, using his home computer and modem. Using the handle "Shadow Hawk," Zinn broke into a Bell Labs computer in Naperville, IL; an AT&T computer in Burlington, NC; and an AT&T computer at Robbins Air Force Base, GA. No classified material was obtained, but the government views as 'highly sensitive' the programs stolen from a computer used by NATO which is tied into the U.S. missile command. In addition, Zinn made unlawful access to a a computer at an IBM facility in Rye, NY, and into computers of Illinois Bell Telephone Company and Rochester Telephone Company, Rochester, NY.

Assistant United States Attorney William Cook said that Zinn obtained access to the AT&T/Illinois Bell computers from computer bulletin board systems, which he described as "...just high-tech street gangs." During his bench trial during January, Zinn spoke in his own defense, saying that he took the programs to educate himself, and not to sell them or share them with other phreaks. The programs stolen included very complex software relating to computer design and artificial intelligence. Also stolen was software used by the BOC's (Bell Operating Companies) for billing and accounting on long distance telephone
~~~~~~~~~~~~~~~~~~~~~~~~~~~

calls.

The Shadow Hawk -- that is, Herbert Zinn, Jr. -- operated undetected for at least a few months in 1986-87, but his undoing came when his urge to brag about his exploits got the best of him. It seems to be the nature of phreaks and hackers that they have to tell others what they are doing. On a BBS notorious for its phreak/pirate messages, Shadow Hawk provided passwords, telephone numbers and technical details of trapdoors he had built into computer systems, including the machine at Bell Labs in Naperville.

What Shadow Hawk did not realize was that employees of AT&T and Illinois Bell love to use that BBS also; and read the messages others have written. Security representatives from IBT and AT&T began reading Shadow Hawk's comments regularly; but they never were able to positively identify him. Shadow Hawk repeatedly made boasts about how he would "shut down AT&T's public switched network." Now AT&T became even more eager to locate him. When Zinn finally discussed the trapdoor he had built into the Naperville computer, AT&T decided to build one of their own for him in return; and within a few days he had fallen into it. Once he was logged into the system, it became a simple matter to trace the telephone call; and they found its origin in the basement of the Zinn family home on North Artesian Street in Chicago, where Herb, Jr. was busy at work with his modem and computer.

Rather than move immediately, with possibly not enough evidence for a good, solid conviction, everyone gave Herb enough rope to hang himself. For over two months, all calls from his telephone were carefully audited. His illicit activities on computers throughout the United States were noted, and logs were kept. Security representatives from Sprint made available notes from their investigation of his calls on their network. Finally the "big day" arrived, and the Zinn residence was raided by FBI agents, AT&T/IBT security representatives and Chicago Police detectives used for backup. At the time of the raid, three computers, various modems and other computer peripheral devices were confiscated. The raid, in September, 1987, brought a crude stop to Zinn's phreaking activities. The resulting newspaper stories brought humiliation and mortification to Zinn's parents; both well-known and respected residents of the Rogers Park neighborhood. At the time of the younger Zinn's arrest, his father spoke with authorities, saying, "Such a good boy! And so intelligent with computers!"

It all came to an end Tuesday morning in Judge Plunkett's courtroom in Chicago, when the judge imposed sentence, placing Zinn in the custody of the Attorney General or his authorized representative for a period of nine months; to be followed by two and a half years federal probation and a $10,000 fine. The judge noted in imposing sentence that, "...perhaps this example will defer others who would make unauthorized entry into computer systems." Accepting the government's claims that Zinn was "simply a burglar; an electronic one... a member of a high-tech street gang," Plunkett added that he hoped Zinn would learn a lesson from this brush with the law, and begin channeling his expert computer ability into legal outlets. The judge also encouraged Zinn to complete his high school education, and "become a contributing member of society instead of what you are now, sir..."

Because Zinn agreed to cooperate with the government at his trial, and at any time in the future when he is requested to do so, the government made no recommendation to the court regarding sentencing. Zinn's attorney asked the court for leniency and a term of probation, but Judge Plunkett felt some incarceration was appropriate. Zinn could have been incarcerated until he reaches the age of 21.

His parents left the courtroom Tuesday with a great sadness. When asked to discuss their son, they said they preferred to make no comment.

Information Collected From Various Sources

_

FBI National Crime Information Center Data Bank   February 13, 1989
~~~~~~
By Evelyn Richards (Washington Post)

"Proposed FBI Crime Computer System Raises Questions on Accuracy, Privacy -- Report Warns of Potential Risk Data Bank Poses to Civil Liberties"

On a Saturday afternoon just before Christmas last year, U.S. Customs officials at Los Angeles International Airport scored a "hit."

Running the typical computer checks of passengers debarking a Trans World Airlines flight from London, they discovered Richard Lawrence Sklar, a fugitive wanted for his part in an Arizona real estate scam.

As their guidelines require, Customs confirmed all the particulars about Sklar with officials in Arizona - his birth date, height, weight, eye and hair color matched those of the wanted man.

Sklar's capture exemplified perfectly the power of computerized crime fighting. Authorities thousands of miles away from a crime scene can almost instantly identify and nab a wanted person.

There was only one problem with the Sklar case: He was the wrong man. The 58-year old passenger - who spent the next two days being strip-searched, herded from one holding pen to another and handcuffed to gang members and other violent offenders - was a political science professor at the University of California at Los Angeles.

After being fingered three times in the past dozen years for the financial trickeries of an impostor, Sklar is demanding that the FBI, whose computer scored the latest hit, set its electronic records straight. "Until this person is caught, I am likely to be victimized by another warrant," Sklar said.

Nowhere are the benefits and drawbacks of computerization more apparent than at the FBI, which is concluding a six-year study on how to improve its National Crime Information Center, a vast computer network that already links 64,000 law enforcement agencies with data banks of 19 million crime-related records.

Although top FBI officials have not signed off on the proposal, the current
~~~~~~

version would let authorities transmit more detailed information and draw on a vastly expanded array of criminal records. It would enable, for example, storage and electronic transmission of fingerprints, photos, tattoos and other physical attributes that might prevent a mistaken arrest. Though controversial, FBI officials have recommended that it include a data bank containing names of suspects who have not been charged with a crime.

The proposed system, however, already has enraged computer scientists and privacy experts who warn in a report that the system would pose a "potentially serious risk to privacy and civil liberties." The report, prepared for the House subcommittee on civil and constitutional rights, also contends that the proposed $40 million overhaul would not correct accuracy problems or assure that records are secure.

Mostly because of such criticism, the FBI's revamped proposal for a new system,
known as the NCIC 2000 plan, is a skeleton of the capabilities first suggested by law enforcement officials. Many of their ideas have been pared back, either
for reasons of practicality or privacy.

"Technical possibility should not be the same thing as permissible policy," said Marc Rotenberg, an editor of the report and Washington liaison for Computer Professionals for Social Responsibility, a California organization. The need to make that tradeoff - to weigh the benefits of technological advances against the less obvious drawbacks - is becoming more apparent as nationwide computer links become the blood vessels of a high-tech society.

Keeping technology under control requires users to double-check the accuracy of
the stored data and sometimes resort told-fashioned paper records or face-to-face contact for confirmation. Errors have plagued the NCIC for many years, but an extensive effort to improve record-keeping has significantly reduced the problem, the FBI said.

Tapped by federal, state and local agencies, the existing FBI system juggles about 10 inquiries a second from people seeking records on wanted persons, stolen vehicles and property, and criminal histories, among other things. Using
the current system, for example, a police officer making a traffic stop can fine out within seconds whether the individual is wanted anywhere else in the United States, or an investigator culling through a list of suspects can peruse
past records.

At one point, the FBI computer of the future was envisioned as having links to a raft of other data bases, including credit records and those kept by the Immigration and Naturalization Service, the Internal Revenue Service, the Social Security Administration and the Securities and Exchange Commission. One by one, review panels have scaled back that plan.

"There's a lot of sensitive information in those data bases," said Lt. Stanley Michaleski, head of records for the Montgomery County [Maryland] police. "I'm not going to tell you that cops aren't going to misuse the information."

The most controversial portion of the planned system would be a major expansion
to include information on criminal suspects - whose guilt has not yet been established.

The proposed system would include names of persons under investigation in

murder, kidnapping or narcotics cases. It would include a so-called "silent hit" feature: An officer in Texas, for instance, would not know that the individual he stopped for speeding was a suspect for murder in Virginia. But when the Virginia investigators flipped on their computer the next morning, it would notify them of the Texas stop. To Michaleski, the proposal sounded like "a great idea. Information is the name of the game." But the "tracking" ability has angered critics.

"That [data base] could be enlarged into all sorts of threats - suspected communists, suspected associates of homosexuals. There is no end once you start," said Rep. Don Edwards (D-Calif.), whose subcommittee called for the report on the FBI's system.

The FBI's chief of technical services, William Bayse, defends the proposed files, saying they would help catch criminals while containing only carefully screened names. "The rationale is these guys are subjects of investigations, and they met a certain guideline," he said.

So controversial is the suspect file that FBI Director William Sessions reportedly may not include it when he publicly presents his plan for a new system.

- -

A case similar to Sklar's was that of Terry Dean Rogan, who was arrested five times because of outstanding warrants caused by someone else masquerading as him. He finally settled for $50,000 in damages.

Legal Clamp-Down On Australian Hackers February 14, 1989

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

By Julie Power (The Financial Review)

Federal Cabinet is expected to endorse today draft legislation containing tough penalties for hacking into Commonwealth computer systems. It is understood that the Attorney-General, Mr. Lionel Bowen, will be proposing a range of tough new laws closely aligned with the recommendations of the Attorney-General's Department released in December. Mr. Bowen requested the report by the Review of Commonwealth Criminal Law, chaired by Sir Harry Gibbs, as a matter of urgency because of the growing need to protect Commonwealth information and update the existing legislation.

Another consideration could be protection against unauthorized access of the tax file number, which will be stored on a number of Government databases.

If the report's recommendations are endorsed, hacking into Commonwealth computers will attract a $48,000 fine and 10 years imprisonment. In addition, it would be an offense to destroy, erase, alter, interfere, obstruct and unlawfully add to or insert data in a Commonwealth computer system.

The legislation does not extend to private computer systems. However, the Attorney-General's Department recommended that it would be an offense to access information held in a private computer via a Telecom communication facility or another Commonwealth communication facility without due authority.

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

Multi-Gigabuck Information Theft   February 8, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
By Bob Mitchell (Toronto Star)(Edited for this presentation)

A man has been arrested and charged with unauthorized use of computer information, following a 2-month police investigation. The suspect was an associate of a "very big" Toronto company: "A company that people would know, with offices across Canada." Police are keeping the company's name secret at its request. They say the perpetrator acted alone.

A password belonging to the company was used to steal information which the company values at $4 billion (Canadian). This information includes computer files belonging to an American company, believed to contain records from numerous companies, and used by large Canadian companies and the United States government.

"We don't know what this individual was planning to do with the information, but the potential is unbelievable. I'm not saying the individual intended to do this, but the program contained the kind of information that could be sold to other companies," said Lewers.

- -

Further investigation of the above details led to the following;

Multi-Gigabuck Value Of Information Theft Denied   February 17, 1989
~~~~~~
Different facts about the information theft were reported two days after the original story.

The information in this article is from the Toronto Globe & Mail. The article is headlined "Computer Information Theft Detected By Security System, Company Says." And it begins as follows:

> "The theft of information from a company's computer program was detected by the firm's own computer security system.
>
> Mike Tillson, president of HCR Corporation, which specializes in developing computer software, said yesterday an unusual pattern of computer access was noticed on the company's system last week."

The article continues by saying that police reports valuing the "program" at $4 billion (Canadian) were called grossly exaggerated by Tilson: "It's more in the tens of thousands of dollars range." He also said that the illegal access had been only a week before; there was no 2-month investigation. And asked about resale of the information, he said, "It's not clear how one would profit from it. There are any number of purposes one could imagine to idle curiosity.
There is a possibility of no criminal intent."

The information not being HCR customer data, and Tilson declining to identify it, the article goes on to mention UNIX, to mumble about AT&T intellectual property, and to note that AT&T is not in the investigation "at this stage."

More Syracuse Busts   February 6, 1989

~~~~~~~~~~~~~~~~~~
St. Elmos Fire was arrested after a supposed friend turned him in to the police
and signed an affidavit. His crimes include hacking into his school's HP3000 and the FBI and Telenet are trying to get him for hacking into another HP3000 system in Illinois.

However, it was the "friend" that was actually the person responsible for the damage done to the computer in Illinois. The problem is that Telenet traced that calls to Syracuse, New York and because of the related crimes, the authorities are inclined to believe that both were done by the same individual.

St. Elmos Fire has already had his arraignment and his lawyer says that there is very little evidence to connect SEF to the HP3000 in Syracuse, NY. However,,
nothing is really known at this time concerning the status of the system in Illinois.

Information Provided by Grey Wizard

Television Editor Charged In Raid On Rival's Files February 8, 1989
~~~~~~
>From San Jose Mercury News

TAMPA, Fla. (AP) - A television news editor hired away from his station by a competitor has been charged with unlawfully entering the computer system of his
former employer to get confidential information about news stories.

Using knowledge of the system to bypass a security shield he helped create, Michael L. Shapiro examined and destroyed files relating to news stories at Tampa's WTVT, according to the charges filed Tuesday.

Telephone records seized during Shapiro's arrest in Clearwater shoed he made several calls last month to the computer line at WTVT, where he worked as assignment editor until joining competitor WTSP as an assistant news editor in October.

Shapiro, 33, was charged with 14 counts of computer-related crimes grouped into
three second-degree felony categories: Offenses against intellectual property,
offenses against computer equipment and offenses against computer users. He was released from jail on his own recognizance.

If convicted, he could be sentenced to up to 15 years in prison and fined $10,000 for each second-degree felony count.

Bob Franklin, WTVT's interim news director, said the station's management discovered several computer files were missing last month, and Shapiro was called to provide help. Franklin said the former employee claimed not to know the cause of the problem.

At a news conference, Franklin said: "Subsequent investigation has revealed that, at least since early January, WTVT's newsroom computer system has been the subject of repeated actual and attempted 'break-ins.' The computers contain highly confidential information concerning the station's current and

future news stories."

The news director said Shapiro was one of two people who had responsibility for
daily operation and maintenance of the computer system after it was installed about eight months ago. The other still works at WTVT.

Terry Cole, news director at WTSP, said Shapiro has been placed on leave of absence from his job. Shapiro did not respond to messages asking for comment.

Franklin said Shapiro, employed by WTVT from February 1986 to September, 1988, left to advance his career. "He was very good at what he did," Franklin said. "He left on good terms."

==Phrack Inc.==

Volume Two, Issue 24, File 13 of 13

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN        P h r a c k   W o r l d   N e w s    PWN
PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~    PWN
PWN                Issue XXIV/Part 3            PWN
PWN                                             PWN
PWN                February 25, 1989            PWN
PWN                                             PWN
PWN          Created, Written, and Edited       PWN
PWN               by Knight Lightning           PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

The Judas Contract Fulfilled! January 24, 1989

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

> "...the other thing that made me mad was that I consider myself, at least I used to consider myself, a person who was pretty careful about who I trust, basically nobody had my home number, and few people even knew where I really lived..."
>
> -The Disk Jockey

The following story, as told by The Disk Jockey, is a prime example of the dangers that exist in the phreak/hack community when sharing trust with those who have made The Judas Contract.

- -

Let me briefly explain how I got caught...

A hacker named Compaq was busted after someone turned him in for using Sprint codes. While executing the search warrant, the state police noticed that he had an excessive amount of computer equipment which had origins that Compaq could not explain.

After checking around (I imagine checking serial numbers that Compaq had not removed), the police found that the equipment was obtained illegally. Compaq then proceeded to tell the police that I, Doug Nelson (as he thought my name was) had brought them to him (true).

Meanwhile, Compaq was talking to me and he told me that he was keeping his mouth shut the entire time. Keep in mind that I had been talking to this guy for quite a long time previously and thought that I knew him quite well. I felt that I was quite a preceptive person.

As time went by, little did I know, Compaq was having meetings again and again with the state police as well as the Federal Bureau of Investigation (FBI) concerning finding out who I was. He gave them a complete description of me, and where I (correctly) went to school, but again, he was SURE my name was Douglas Nelson, and since my phone had previously been in that name, he felt assured that he was correct. The Police checked with Illinois and couldn't find license plates or a driver's license in that name. He had remembered seeing Illinois license plates on my car.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

They were stuck until Compaq had a wonderful: He and I had went out to dinner and over the course of conversation, I mentioned something about living in Bloomfield Hills, Michigan.

After telling the state police this information, they wrote to Bloomfield Hills
and gave a description and asked for any pictures in their files that fit that description.

The problem was that several years ago, some friends and I were arrested for joyriding in a friend's snowmobile while he was on vacation. The neighbors didn't know us and called the police. Charges were dropped, but our prints and
pictures were on file.

Bloomfield Hills sent back 12 pictures, which, according to the police report, "Kent L. Gormat (Compaq) without hesitation identified picture 3 as the individual he knows as Douglas Nelson. This individuals name was in fact Douglas..."

A warrant was issued for me and served shortly afterwards by state, local and federal authorities at 1:47 AM on June 27, 1988.

Lucky me to have such a great pal. In the 6 months that I was in prison, my parents lived 400 miles away and couldn't visit me, my girlfriend could come visit me once a month at best, since she was so far away, and Compaq, who lived
a whole 10 miles away, never came to see me once. This made me rather angry as
I figured this "friend" had a lot of explaining to do.

As you can see I am out of prison now, but I will be on probation until December 15, 1989.

-The Disk Jockey

Bogus Frequent Flyer Scheme February 13, 1989

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

>From Associated Press

An airline ticket agent piled up 1.7 million bonus air miles via computer without leaving the ground, then sold the credits for more than $20,000, according to a published report.

Ralf Kwaschni, age 28, was arrested Sunday when he arrived for work at Kennedy International Airport and was charged with computer tampering and grand larceny, authorities said.

Kwaschni, a ticket agent for Lufthansa Airlines, used to work for American Airlines. Police said he used his computer access code to create 18 fake American Airline Advantage Accounts - racking up 1.7 million bonus air miles, according to the newspaper.

All 18 accounts, five in Kwaschni's name and 13 under fake ones, listed the same post office box, according to the newspaper.

Instead of exchanging the bonus miles for all the free travel, Kwaschni sold some of them for $22,500 to brokers, who used the credits to get a couple of first class, round trip tickets from New York to Australia, two more between
~~~~~~~~~~~~~~~~~~~~~~~~~~

London and Bermuda, and one between New York and Paris. It is legal to sell personal bonus miles to brokers Port Authority Detective Charles Schmidt said.

Kwaschni would create accounts under common last names. When a person with one of the names was aboard an American flight and did not have an Advantage account, the passengers name would be eliminated from the flight list and replaced with one from the fake accounts.

"As the plane was pulling away from the gate, this guy was literally wiping out passengers," Schmidt said.

Massive Counterfeit ATM Card Scheme Foiled February 11, 1989

By Douglas Frantz (Los Angeles Times)

The U.S. Secret Service foiled a scheme to use more than 7,700 counterfeit ATM cards to obtain cash from Bank of America automated tellers. After a month-long investigation with an informant, five people were arrested and charged with violating federal fraud statutes.

"Seized in the raid were 1,884 completed counterfeit cards, 4,900 partially completed cards, and a machine to encode the cards with Bank Of America account information, including highly secret personal identification numbers for customers."

The alleged mastermind, Mark Koenig, is a computer programmer for Applied Communications, Inc. of Omaha, a subsidiary of U.S. West. He was temporarily working under contract for a subsidiary of GTE Corporation, which handles the company's 286 ATMs at stores in California. Koenig had access to account information for cards used at the GTE ATMs. According to a taped conversation, Koenig said he had transferred the BofA account information to his home computer. He took only Bank Of America information "to make it look like an inside job" at the bank. The encoding machine was from his office.

Koenig and confederates planned to spread out across the country over six days around the President's Day weekend, and withdraw cash. They were to wear disguises because some ATMs have hidden cameras. Three "test" cards had been used successfully, but only a small amount was taken in the tests, according to the Secret Service.

The prosecuting US attorney estimated that losses to the bank would have been between $7 and $14 million. Bank Of America has sent letters to 7,000 customers explaining that they will receive new cards.

STARLINK - An Alternative To PC Pursuit January 24, 1989

STARLINK is an alternative to PC Pursuit. You can call 91 cities in 28 states during off-peak hours (7pm-6am and all weekend) for $1.50 per hour. All connections through the Tymnet network are 2400 bps (1200 bps works too) with no surcharge and there are no maximum hours or other limitations.

There is a one time charge of $50 to signup and a $10 per month account maintenance fee. High volume users may elect to pay a $25 per month maintenance fee and $1.00 per hour charge.

The service is operated by Galaxy Telecomm in Virginia Beach, VA and users may sign up for the service by modem at 804-495-INFO. You will get 30 minutes free
access time after signing up.

This is a service of Galaxy and not TYMNET. Galaxy buys large blocks of hours from TYMNET. To find out what your local access number is you can call TYMNET at (800) 336-0149 24 hours per day. Don't ask them questions about rates, etc., as they don't know. Call Galaxy instead.

Galaxy says they will soon have their own 800 number for signups and information.

The following is a listing of the major cities covered. There are others that are a local call from the ones listed.

Eastern Time Zone

Connecticut: Bloomfield Hartford Stamford
Florida: Fort Lauderdale Jacksonville Longwood Miami Orlando Tampa
Georgia: Atlanta Doraville Marietta Norcross
Indiana: Indianapolis
Maryland: Baltimore
Massachusetts: Boston Cambridge
New Jersey: Camden Englewood Cliffs Newark Pennsauken Princeton South Brunswick
New York: Albany Buffalo Melville New York Pittsford Rochester White Plains
North Carolina: Charlotte
Ohio: Akron Cincinnati Cleveland Columbus Dayton
Pennsylvania: Philadelphia Pittsburgh
Rhode Island: Providence
Virginia: Alexandria Arlington Fairfax Midlothian Norfolk Portsmouth

Central Time Zone

Alabama: Birmingham
Illinois: Chicago Glen Ellyn
Kansas: Wichita
Michigan: Detroit
Minnesota: Minneapolis St. Paul
Missouri: Bridgeton Independence Kansas City St. Louis
Nebraska: Omaha
Oklahoma: Oklahoma City Tulsa
Tennessee: Memphis Nashville
Texas: Arlington Dallas Fort Worth Houston
Wisconsin: Brookfield Milwaukee

Mountain Time Zone

Arizona: Mesa Phoenix Tucson
Colorado: Aurora Boulder Denver

Pacific Time Zone

California: Alhambra Anaheim El Segundo Long Beach Newport Beach
Oakland Pasadena Pleasanton Sacramento San Francisco
San Jose Sherman Oaks Vernon Walnut Creek
Washington: Bellevue Seattle

STARLINK is a service of Galaxy Telecomm Division, GTC, Inc., the publishers of
BBS Telecomputing News, Galaxy Magazine and other electronic publications.

Suspended Sentences For Computer Break-In February 20, 1989
~~~~~~
>From Personal Computing Weekly

"Police Officers Sentenced For Misuse Of Police National Computer"

Three police officers hired by private investigators to break into the Police National Computer received suspended prison sentences at Winchester Crown Court. The private investigators also received suspended (prison) sentences, ranging from four to six months.

The police officers were charged under the Official Secrets Act of conspiring to obtain confidential information from the Police National Computer at Hendon.

One of the police officers admitted the charge, but the other two and the private investigators pleaded Not Guilty.

The case arose out of a Television show called "Secret Society" in which private investigator Stephen Bartlett was recorded telling journalist Duncan Campbell that he had access to the Police National Computer, the Criminal Records Office at Scotland Yard and the DHSS (Department of Health & Social Security).

Bartlett said he could provide information on virtually any person on a few hours. He said he had the access through certain police officers at Basingstoke, Hampshire. Although an investigation proved the Basingstoke connection to be false, the trail led to other police officers and private detectives elsewhere.

Most of the information gleaned from the computers was used to determine who owned certain vehicles, who had a good credit record -- or even who had been in
a certain place at a certain time for people investigating marital infidelity.

- -
Of course, the actions for which the officers and others were sentenced, were not computer break-ins as such, but rather misuse of legitimate access.

Virus Hoax Caused As Much Panic As The Real Thing February 20, 1989
~~~~~~

>From Popular Computing Weekly

"A Virus Is Up And Running"

Michael Banbrook gave his college network managers a scare when he planted a message saying that a virus was active on the college system.

Banbrook's message appeared whenever a user miskeyed a password; the usual message would be

"You are not an authorized user."

It was replaced by the brief but sinister:

"A Virus is up and running."

When the message was discovered by the college network manager, Banbrook was immediately forbidden access to any computers at the St. Francix Xavier College
at Clapham in South London.

Banbrook, 17, told "Popular Computing Weekly" that he believed the college has over-reacted and that he had, in fact thrown a spotlight on the college's lackluster network security. The college has a 64 node RM Nimbus network running MS-DOS.

"All any has to do is change a five-line DOS batch file" says Banbrook. "There is no security at all"

Banbrook admits his motives were not entirely related to enhancing security: "I was just bored and started doodling and where some people would doodle with a notepad, I doodle on a keyboard. I never thought anyone would believe the message."

Banbrook was suspended from computer science A-level classes and forbidden to use the college computers for a week before it was discovered that no virus existed. Following a meeting between college principal Bryan Scalune and Banbrook's parents, things are said to be "back to normal."

Phrack World News -- Quicknotes
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

For those interested in the 312/708 NPA Split, the correct date for this division is November 11, 1989. However, permissive dialing will continue until
at least February 9, 1990.

Anyone who is wondering what Robert Morris, Jr. looks like should have a look at Page 66 in the January 1989 issue of Discover Magazine.

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