==Phrack Inc.==

Volume Three, Issue 29, File #1 of 12

Phrack Inc. Newsletter Issue XXIX Index
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
November 17, 1989

     Greetings and welcome to Issue 29 of Phrack Inc. For those of you who
have been with us from the beginning, the date on this issue may hold some
historical significance:

          Happy Fourth Anniversary Phrack Inc.!

     This issue we feature two files dealing with electronic fund transfer
written by a member of the Legion of Doom who wishes to remain anonymous.
The second article tells a story detailing how an actual electronic fund
transfer might take place -- Is it true or is it fiction? We decided to let
you, the reader, decide that for yourself.

     The Future Transcendent Saga continues as usual in this issue with part
two of "Introduction to the Internet Protocols." We also present to you the
second edition of Network Miscellany which focuses largely on Public Access
Unix systems around the country. Last, but not least, concerning the wide area
networks, we have Covert Paths -- a file about hacking on the Internet and how
to make sure you cannot be tracked down.

     On a lighter note, it appears that Teleconnect Magazine liked The Mentor's
"Hacker's Manifesto" so much that they decided to print a portion of it in
their November 1989 issue. If you receive this magazine you will find it on
page 55, but only the last 4 paragraphs (they apparently did not like the
beginning of the file). The interesting thing is that Teleconnect claims that
they were given the article by MCI Security who recently discovered it on a
bulletin board. If you are a long time reader of Phrack Inc., you might
remember that this article was dated for January 8, 1986 and originally
appeared in Phrack Inc. Newsletter Issue VII (file 3 of 10) and again in issue
XXIV (file 3 of 9).

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

          Taran King   Knight Lightning
       C488869@UMCVMB.BITNET   C483307@UMCVMB.BITNET
     C488869@UMCVMB.MISSOURI.EDU   C483307@UMCVMB.MISSOURI.EDU

And we can also be reached via our new mail forwarding addresses (for those
that cannot mail to our Bitnet or Internet addresses):

          ...!netsys!phrack   or   phrack@netsys.COM
_____

Table of Contents:

_____
          >-----------=====END=====----------<

                        ==Phrack Inc.==

               Volume Three, Issue 29, File #2 of 12

                     ==Phrack Pro-Phile XXIX==

                  Created and Presented by Taran King

                     Done on November 12, 1989

        Welcome to Phrack Pro-Phile XXIX. Phrack Pro-Phile was created to
bring information to you, the community, about retired or highly important/
controversial people. This edition of the Phrack Pro-Phile starts a different
format as I'm sure you will notice. The skeleton of the Pro-Phile is a form
in which the people fill in the blanks. Starting now, using their words (and a
little editing), the Pro-Phile will be presented in first person format. This
month, we present to you the editor of one of the most prominent printed
phreak/hack newsletters of all times...

                        Emmanuel Goldstein
                        ~~~~~~~~~~~~~~~~~~~

             Handle: Emmanuel Goldstein
           Call Him: Call me anything. Just look me in the eye.
      Past Handles: Howard Tripod, Sidney Schreiber, Bob Hardy, Gary Wilson,
                     Clint Eastwood, 110. There are others that I keep quiet
                     about.
     Handle Origin: I prefer using regular names rather than descriptive
                     boastful titles (i.e., "The Hacker King," who,
                     incidentally, I don't wish to offend if he/she even exists;
                     this is just an example). The names I use are either
                     people I've "become" or names that bestow a certain image.
                     Emmanuel Goldstein, for instance, led the resistance in
                     "1984." But then, there was talk that he never really
                     existed and was just created by the government in order to
                     capture the real subversives. I don't think that's the
                     case with me.
          Computers: I use PC compatibles for the most part. I also play around
                     with Macs but they're not REAL computers to me. My
                     favorite machine of all time is the Zenith Z-100, a
                     dual-processor computer that can emulate an old fashioned
                     H8 or an IBM PC. It runs lots of operating systems and has
                     a great keyboard. Too bad it was discontinued four years
                     ago....
Sysop/Co-Sysop Of: The old Plovernet on Long Island (1984), Private Sector in
                     New Jersey (1985, 1986), and the present and future 2600
                     boards.

Origins in Phreak/Hack World
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
I've been playing with phones all of my life and I started playing with
computers the first time I saw one. I always seemed to get in trouble for
doing things I wasn't supposed to... crashing the PDP-10 in high school...
flashing the switchhook on my phone 95 times and getting an angry switchman who
wouldn't release the line, claiming I broke it (I was 10). As computers and
phones started to become integrated, I realized what hacking really was -- just
asking a lot of questions and being really persistent. A lot of people don't
like that, whether it's computers or real life, but how else are you going to
learn what's REALLY happening and not just what others WANT you to know?

Origins in Phreak/Hack BBSes
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
I don't really have a BBS reputation to speak of. They tend to disappear
rather quickly and that tends to dampen my enthusiasm towards them quite a bit,
but I do want to see more and more of them come up and begin to reach out and
be creative. They also have to challenge the system some more. 2600 has a
very strong opinion on BBS privacy, namely that the same rights afforded to any
publication should be extended to a bulletin board, but every BBS owner should
know the importance of this and should be willing to fight for it. If you
didn't believe in preserving the First Amendment, you probably wouldn't go out

and buy a newspaper, would you? A BBS is the same thing and anyone who runs a
system should see this connection. Hackers tend to bring this issue to the
forefront a bit more, but this is something that applies to all bulletin
boards.

Encounters With Phreakers and Hackers
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Meeting Captain Crunch in Amsterdam this past summer was a real trip. Finding
out who Cable Pair really was certainly resulted in some highlights. I've met
a lot of "famous" phreaks and hackers and now I know a lot of foreign ones, but
I'm always amazed at the number of people I meet (mostly in New York) who say
they've been hacking since the sixties. There's an awful lot of people out
there who are into this kind of stuff, which is something I never knew before I
started being open about these particular interests.

Experience Gained In The Following Ways
~~~~~~
Social engineering, of course. I like hacking computers when I'm not feeling
social because you don't have to adjust your attitude to get a reply, but
people hacking is so much more satisfying. No matter how many security codes
and precautions are taken, as long as one person without knowledge is able to
talk to another with knowledge, it will always be possible to get things out of
them. Most of the really important bits of information I've been able to get
are through people, not computers.

Knowledge Attributed To...
~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Ignorance. I built up my knowledge by wandering around in places others
thought unimportant. Hacking can be like trashing. It looks like garbage or a
waste of time to most, but if you keep your mind open, you can learn a lot. If
more people felt this way, hackers would stand out less because everyone would
be a bit more adventurous, but ignorance prevails and we learn what nobody else
cares about...that is until it affects them.

Work/Schooling
~~~~~~~~~~~~~~~
I got an English degree at Stony Brook (it's currently gathering dust in a
closet). I should note that I've never taken a computer course, nor do I
intend to. I've worked as a limo driver, a Good Humor man, and a typesetter,
and more recently, as a freelance writer, a reporter for Pacifica Radio, and a
radio engineer/producer and talk show host.

Busted For...
~~~~~~~~~~~~~~
I used to make free phone calls all the time. Now, obviously, I can't do that,
since I'm in the public eye, but that's not a drawback to me because I can
still experiment all I want. Nothing can change that. For the most part I was
careful while I was doing these things, but there was one time when my luck ran
out. I had been using Telemail to communicate with some other people and they,
unknown to us, had been looking for hackers on their system. They found us,
the members of PHALSE (Phreakers, Hackers, and Laundromat Service Employees
[I'm told the feds spent a lot of time investigating the laundry connection,
even though we only used it to spell out the word PHALSE!]). I believe four
people got indicted in that adventure. I was one of them. Bill Landreth was
another. They thought I was the ringleader so they gave me a 10 count
indictment, more than twice what anyone else got. Without hiring an expensive
lawyer, I talked to a roomful of feds about the system and what was wrong with
it. I made it clear that I wasn't turning anybody in -- even if I wanted to I
still didn't know who or where they were. I think I was dealt with fairly. I
told them what I did and paid for the time I used. Nothing more. That was in
1984 when 2600 was just getting off the ground. A couple of years ago, one of
the feds who had questioned me tried to get me to work for them. Not to entrap
hackers, but Soviet spies. And so it goes.

Interests
~~~~~~~~~~
I guess I'm an explorer because everything I like doing involves exploration of
some sort. Obviously, hacking contains a good amount of that. I like
traveling quite a bit, particularly when I'm free to do whatever the hell I
want. Traveling with people is fun but it can also be a drag because something

you want to do puts them off and then you either wind up not doing it or doing
it and pissing them off. I like to ride subways to weird places and walk
through bad neighborhoods. It's all a part of exploring and seeing the world
through different eyes. A couple of years ago I went to Baffin Island and hung
out for a week with Eskimos. Everyone thought I was crazy but I had a great
time. I'm also into astronomy, but not the classroom kind. I took a course
in astronomy once and it was the biggest mistake of my life. All we did was
talk about equations. I like to look at the sky and read about what's being
discovered up there. When the space telescope goes up next year, interest in
space will rise again. Then there's free-lance writing, which I have to devote
more time to. I'm working on a couple of plays, some short stories, a
screenplay for a movie, and a screenplay for TV. I'll probably focus on the
plays only because there's so much bullshit involved in TV and movies. And
finally, there's radio. I've been in radio for just over 10 years, doing
whatever comes to mind on WUSB-FM in Stony Brook, NY, a small, noncommercial
radio station at the State University. Now I also work at WBAI-FM, a much
larger station in New York City with the same kind of free-form attitude.
There's so much you can do with radio, but so few stations want to take a
chance any more. That's why they all sound the same. Unfortunately, when you
sell commercials, you also sell your freedom. I've seen it enough times to
know it's true and that's the reason I've stayed out of commercial radio.
Right now I do a weekly talk show on WUSB called "Brain Damage" where I take
calls, play with the phones, and air tapes from Radio Moscow. On WBAI I'm
doing two shows: "News of the World" which is a compilation of foreign news
reports and "Off The Hook," a program about, you guessed it, phone phreaks.

Favorite Things
~~~~~~~~~~~~~~~~

I like hanging out with fun people who are open-minded, non-judgmental, and
preferably insane to a degree. I enjoy talking on the phone with friends and
strangers alike. Strangers are different because you can be whoever you want
to be with them. They tend to believe almost anything you say. Music is
really important. Right now I like rappers and toasters the most, with soca
and hardcore close behind. Ska's real good too, but there's not much coming
out. The record I put on when I wake up sets my mood for the day. I like
music with lyrics that mean something. There's a time and a place for mindless
droning but there's too much of it around. Music should have meaning. In
Jamaica, people don't buy newspapers. They buy records and that's how they
learn what's going on and what the latest catch phrases are. Some of my
favorite rock bands include The Clash, Big Audio Dynamite, Dead Kennedys,
Donner Party, Public Enemy, Camper Van Beethoven, Pink Floyd, Fun Boy Three, De
La Soul, and Anti-Nowhere League. Some of my favorite solo artists are Tracy
Chapman, John Lennon, Elvis Costello, and Patsy Cline. I realize I'm very
lucky because I work in an environment (noncommercial radio station) that gets
over 100 new albums a week. I don't know how I would have ever found some of
the stuff I like if I didn't have that kind of access.

Inside Jokes
~~~~~~~~~~~~~

 "OK, if we can't have a tour, can we at least have a look around?"

 "I'm not allowed to talk to you any more."

 "This is the Sprint operator. I have a collect call from AT&T."

 "There aren't any more supervisors, sir. You've spoken to all of them."

 "Iran, will you hang up! Sir, do you speak what he speaks?"

 "I said, DON'T hit return!"

 "But we didn't know it was the foreign minister!"

 "Repair serv-- damn! There it goes again. What the hell's wrong with
   these phones?"

 "Just tell me how much money you lost and I'll arrange for a trial date."

Serious Section
~~~~~~~~~~~~~~~~

Being a part of the hack/phreak community, you get to experience unique little
adventures that the "average" person has no conception of. We talk to people
over the phone and have no idea what they look like, often no idea what they
even sound like (BBSes). We play with technology and are thought of as
geniuses merely because the rest of the world doesn't understand what we're
doing. I think that goes to our heads sometimes, which is bad for everyone.
We should apply our knowledge and skills not only to help ourselves by getting
a high-paying job somewhere but to help others as well. Look what happened in
China. Using FAX machines, modems, and redial functions, people forced
information into the country and tied up the government's snitch lines which
probably saved a few lives. The "average" person would never think of applying
technology in this way, but we do and we know how to do it efficiently,
quickly, and without spending money. It's because of that last one that we've
got freedom. Most people don't do things because of the cost. Without having
to worry about that, you can be a lot more imaginative. Of course, that also
makes it illegal, which is enough to stifle some of us. What we do and how we
do it is a decision we each have to make, but we should stop wasting time
boasting and get on with the exploring and the learning and the new
applications. Another thing that really gets me is the person who says,
"hacking and phreaking isn't what it used to be." First off, if nothing
changes, life gets pretty dull. Second, that statement is usually a precursor
to something like, "what kids do today isn't real hacking. What I did 5, 10,
20 years ago was REAL hacking." Generalizations like that are worthless. It's
just like yuppies going on about the Beatles, calling that real music, and
saying the sounds of today are crap (by the way, I like the Beatles a lot). At
the same time, too many hackers are just starting out and thinking they know it
all, dismissing everything that happened before they were around. The spirit
of today's hacker is often the same as that of a phone phreak of the sixties.
And there were people like us around 100 years ago but we're even more far
removed from what they could have possibly been doing. The point is that
there's a bond that ties a lot of us together -- it cuts through time and
backgrounds. Like anything else, there's too much hypocrisy and judging going
on in the hack/phreak world. I think it's a real waste of time.

Are Phreaks/Hackers You've Met Generally Computer Geeks?
~~~~~~

Not in the least. Those people that I've come to know have turned out to be
just about everything you can imagine. White/Black, Jew/Gentile, straight/gay,
male/female, opened/closed, you name it. Everyone's got different sides to
them, stuff they don't always want others to know. Sometimes we try to squash
those other sides of us, but they still exist. I've met hackers who have
geekish qualities but once you get to know them, you realize there's more to
them. Of course, there are lots of hackers I would never want to know in a
million years; that's just the way I am with a lot of people. I think it was
Linus Van Pelt who said, "I love mankind. It's people I can't stand."

>-----------=====END============-----<

                        ==Phrack Inc.==

              Volume Three, Issue 29, File #3 of 12

        <><><><><><><><><><><><><><><><><><><><><><><><><><><>
        <>   <>
        <>   Introduction to the Internet Protocols <>
        <>   ~~~~~~ <>
        <>   Chapter Nine Of The Future Transcendent Saga <>
        <>   <>
        <>   Part Two of Two Files   <>
        <>   <>
        <>   Presented by Knight Lightning   <>
        <>   September 27, 1989   <>
        <>   <>
        <><><><><><><><><><><><><><><><><><><><><><><><><><><>

Prologue - Part Two
~~~~~~~~~
A great deal of the material in this file comes from "Introduction to the
Internet Protocols" by Charles L. Hedrick of Rutgers University. That material
is copyrighted and is used in this file by permission. Time differention and
changes in the wide area networks have made it neccessary for some details of
the file to updated and in some cases reworded for better understanding by our
readers. Also, Unix is a trademark of AT&T Technologies, Inc. -- Again, just
thought I'd let you know.

Table of Contents - Part Two
~~~~~~~~~~~~~~~~~~
*   Introduction - Part Two
*   Well Known Sockets And The Applications Layer
*   Protocols Other Than TCP: UDP and ICMP
*   Keeping Track Of Names And Information: The Domain System
*   Routing
*   Details About The Internet Addresses: Subnets And Broadcasting
*   Datagram Fragmentation And Reassembly
*   Ethernet Encapsulation: ARP
*   Getting More Information

Introduction - Part Two
~~~~~~~~~~~~~
This article is a brief introduction to TCP/IP, followed by suggestions on
what to read for more information. This is not intended to be a complete
description, but it can give you a reasonable idea of the capabilities of the
protocols. However, if you need to know any details of the technology, you
will want to read the standards yourself.

Throughout this file, you will find references to the standards, in the form of
"RFC" (Request For Comments) or "IEN" (Internet Engineering Notes) numbers --
these are document numbers. The final section (Getting More Information)
explains how you can get copies of those standards.

Well-Known Sockets And The Applications Layer
~~~~~~
In part one of this series, I described how a stream of data is broken up into
datagrams, sent to another computer, and put back together. However something
more is needed in order to accomplish anything useful. There has to be a way
for you to open a connection to a specified computer, log into it, tell it what
file you want, and control the transmission of the file. (If you have a
different application in mind, e.g. computer mail, some analogous protocol is
needed.) This is done by "application protocols." The application protocols
run "on top" of TCP/IP. That is, when they want to send a message, they give
the message to TCP. TCP makes sure it gets delivered to the other end.
Because TCP and IP take care of all the networking details, the applications
protocols can treat a network connection as if it were a simple byte stream,
like a terminal or phone line.

Before going into more details about applications programs, we have to describe
how you find an application. Suppose you want to send a file to a computer
whose Internet address is 128.6.4.7. To start the process, you need more than
just the Internet address. You have to connect to the FTP server at the other
end. In general, network programs are specialized for a specific set of tasks.
Most systems have separate programs to handle file transfers, remote terminal
logins, mail, etc. When you connect to 128.6.4.7, you have to specify that you
want to talk to the FTP server. This is done by having "well-known sockets"
for each server. Recall that TCP uses port numbers to keep track of individual
conversations. User programs normally use more or less random port numbers.
However specific port numbers are assigned to the programs that sit waiting for
requests. For example, if you want to send a file, you will start a program
called "ftp." It will open a connection using some random number, say 1234,
for the port number on its end. However it will specify port number 21 for the
other end. This is the official port number for the FTP server. Note that
there are two different programs involved. You run ftp on your side. This is
a program designed to accept commands from your terminal and pass them on to
the other end. The program that you talk to on the other machine is the FTP
server. It is designed to accept commands from the network connection, rather
than an interactive terminal. There is no need for your program to use a
well-known socket number for itself. Nobody is trying to find it. However the
servers have to have well-known numbers, so that people can open connections to
them and start sending them commands. The official port numbers for each
program are given in "Assigned Numbers."

Note that a connection is actually described by a set of 4 numbers: The
Internet address at each end, and the TCP port number at each end. Every
datagram has all four of those numbers in it. (The Internet addresses are in
the IP header, and the TCP port numbers are in the TCP header.) In order to
keep things straight, no two connections can have the same set of numbers.
However it is enough for any one number to be different. For example, it is
perfectly possible for two different users on a machine to be sending files to
the same other machine. This could result in connections with the following
parameters:

```
                    Internet addresses          TCP ports
      connection 1  128.6.4.194, 128.6.4.7      1234, 21
      connection 2  128.6.4.194, 128.6.4.7      1235, 21
```

Since the same machines are involved, the Internet addresses are the same.
Since they are both doing file transfers, one end of the connection involves
the well-known port number for FTP. The only thing that differs is the port
number for the program that the users are running. That's enough of a
difference. Generally, at least one end of the connection asks the network
software to assign it a port number that is guaranteed to be unique. Normally,
it's the user's end, since the server has to use a well-known number.

Now that we know how to open connections, let's get back to the applications
programs. As mentioned earlier, once TCP has opened a connection, we have
something that might as well be a simple wire. All the hard parts are handled
by TCP and IP. However we still need some agreement as to what we send over
this connection. In effect this is simply an agreement on what set of commands
the application will understand, and the format in which they are to be sent.
Generally, what is sent is a combination of commands and data. They use
context to differentiate. For example, the mail protocol works like this:
Your mail program opens a connection to the mail server at the other end. Your
program gives it your machine's name, the sender of the message, and the
recipients you want it sent to. It then sends a command saying that it is
starting the message. At that point, the other end stops treating what it sees
as commands, and starts accepting the message. Your end then starts sending
the text of the message. At the end of the message, a special mark is sent (a
dot in the first column). After that, both ends understand that your program
is again sending commands. This is the simplest way to do things, and the one
that most applications use.

File transfer is somewhat more complex. The file transfer protocol involves
two different connections. It starts out just like mail. The user's program
sends commands like "log me in as this user," "here is my password," "send me
the file with this name." However once the command to send data is sent, a
second connection is opened for the data itself. It would certainly be

possible to send the data on the same connection, as mail does. However file
transfers often take a long time. The designers of the file transfer protocol
wanted to allow the user to continue issuing commands while the transfer is
going on. For example, the user might make an inquiry, or he might abort the
transfer. Thus the designers felt it was best to use a separate connection for
the data and leave the original command connection for commands. (It is also
possible to open command connections to two different computers, and tell them
to send a file from one to the other. In that case, the data couldn't go over
the command connection.)

Remote terminal connections use another mechanism still. For remote logins,
there is just one connection. It normally sends data. When it is necessary to
send a command (e.g. to set the terminal type or to change some mode), a
special character is used to indicate that the next character is a command. If
the user happens to type that special character as data, two of them are sent.

I am not going to describe the application protocols in detail in this file.
It is better to read the RFCs yourself. However there are a couple of common
conventions used by applications that will be described here. First, the
common network representation: TCP/IP is intended to be usable on any
computer. Unfortunately, not all computers agree on how data is represented.

There are differences in character codes (ASCII vs. EBCDIC), in end of line
conventions (carriage return, line feed, or a representation using counts), and
in whether terminals expect characters to be sent individually or a line at a
time. In order to allow computers of different kinds to communicate, each
applications protocol defines a standard representation. Note that TCP and IP
do not care about the representation. TCP simply sends octets. However the
programs at both ends have to agree on how the octets are to be interpreted.

The RFC for each application specifies the standard representation for that
application. Normally it is "net ASCII." This uses ASCII characters, with end
of line denoted by a carriage return followed by a line feed. For remote
login, there is also a definition of a "standard terminal," which turns out to
be a half-duplex terminal with echoing happening on the local machine. Most
applications also make provisions for the two computers to agree on other
representations that they may find more convenient. For example, PDP-10's have
36-bit words. There is a way that two PDP-10's can agree to send a 36-bit
binary file. Similarly, two systems that prefer full-duplex terminal
conversations can agree on that. However each application has a standard
representation, which every machine must support.

So that you might get a better idea of what is involved in the application
protocols, here is an imaginary example of SMTP (the simple mail transfer
protocol.) Assume that a computer called FTS.PHRACK.EDU wants to send the
following message.

    Date: Fri, 17 Nov 89 15:42:06 EDT
    From: knight@fts.phrack.edu
    To: taran@msp.phrack.edu
    Subject: Anniversary

    Four years is quite a long time to be around. Happy Anniversary!

Note that the format of the message itself is described by an Internet standard
(RFC 822). The standard specifies the fact that the message must be
transmitted as net ASCII (i.e. it must be ASCII, with carriage return/linefeed
to delimit lines). It also describes the general structure, as a group of
header lines, then a blank line, and then the body of the message. Finally, it
describes the syntax of the header lines in detail. Generally they consist of
a keyword and then a value.

Note that the addressee is indicated as TARAN@MSP.PHRACK.EDU. Initially,
addresses were simply "person at machine." Today's standards are much more
flexible. There are now provisions for systems to handle other systems' mail.
This can allow automatic forwarding on behalf of computers not connected to the
Internet. It can be used to direct mail for a number of systems to one central
mail server. Indeed there is no requirement that an actual computer by the
name of FTS.PHRACK.EDU even exist (and it doesn't). The name servers could be
set up so that you mail to department names, and each department's mail is

routed automatically to an appropriate computer. It is also possible that the
part before the @ is something other than a user name. It is possible for
programs to be set up to process mail. There are also provisions to handle
mailing lists, and generic names such as "postmaster" or "operator."

The way the message is to be sent to another system is described by RFCs 821
and 974. The program that is going to be doing the sending asks the name
server several queries to determine where to route the message. The first
query is to find out which machines handle mail for the name FTS.PHRACK.EDU.
In this case, the server replies that FTS.PHRACK.EDU handles its own mail. The
program then asks for the address of FTS.PHRACK.EDU, which for the sake of this
example is is 269.517.724.5. Then the the mail program opens a TCP connection
to port 25 on 269.517.724.5. Port 25 is the well-known socket used for
receiving mail. Once this connection is established, the mail program starts
sending commands. Here is a typical conversation. Each line is labelled as to
whether it is from FTS or MSP. Note that FTS initiated the connection:

```
     MSP     220 MSP.PHRACK.EDU SMTP Service at 17 Nov 89 09:35:24 EDT
     FTS     HELO fts.phrack.edu
     MSP     250 MSP.PHRACK.EDU - Hello, FTS.PHRACK.EDU
     FTS     MAIL From:<knight@fts.phrack.edu>
     MSP     250 MAIL accepted
     FTS     RCPT To:<taran@msp.phrack.edu>
     MSP     250 Recipient accepted
     FTS     DATA
     MSP     354 Start mail input; end with <CRLF>.<CRLF>
     FTS     Date: Fri, 17 Nov 89 15:42:06 EDT
     FTS     From: knight@fts.phrack.edu
     FTS     To: taran@msp.phrack.edu
     FTS     Subject: Anniversary
     FTS
     FTS     Four years is quite a long time to be around.  Happy Anniversary!
     FTS     .
     MSP     250 OK
     FTS     QUIT
     MSP     221 MSP.PHRACK.EDU Service closing transmission channel
```

The commands all use normal text. This is typical of the Internet standards.
Many of the protocols use standard ASCII commands. This makes it easy to watch
what is going on and to diagnose problems. The mail program keeps a log of
each conversation so if something goes wrong, the log file can simply be mailed
to the postmaster. Since it is normal text, he can see what was going on. It
also allows a human to interact directly with the mail server, for testing.

The responses all begin with numbers. This is also typical of Internet
protocols. The allowable responses are defined in the protocol. The numbers
allow the user program to respond unambiguously. The rest of the response is
text, which is normally for use by any human who may be watching or looking at
a log. It has no effect on the operation of the programs. The commands
themselves simply allow the mail program on one end to tell the mail server the
information it needs to know in order to deliver the message. In this case,
the mail server could get the information by looking at the message itself.

Every session must begin with a HELO, which gives the name of the system that
initiated the connection. Then the sender and recipients are specified. There
can be more than one RCPT command, if there are several recipients. Finally
the data itself is sent. Note that the text of the message is terminated by a
line containing just a period, but if such a line appears in the message, the
period is doubled. After the message is accepted, the sender can send another
message, or terminate the session as in the example above.

Generally, there is a pattern to the response numbers. The protocol defines
the specific set of responses that can be sent as answers to any given command.
However programs that don't want to analyze them in detail can just look at the
first digit. In general, responses that begin with a 2 indicate success.
Those that begin with 3 indicate that some further action is needed, as shown
above. 4 and 5 indicate errors. 4 is a "temporary" error, such as a disk
filling. The message should be saved, and tried again later. 5 is a permanent
error, such as a non-existent recipient. The message should be returned to the
sender with an error message.

For more details about the protocols mentioned in this section, see RFCs
821/822 for mail, RFC 959 for file transfer, and RFCs 854/855 for remote
logins. For the well-known port numbers, see the current edition of Assigned
Numbers, and possibly RFC 814.

Protocols Other Than TCP: UDP and ICMP
~~~~~~
Thus far only connections that use TCP have been described. Remember that TCP
is responsible for breaking up messages into datagrams, and reassembling them
properly. However in many applications, there are messages that will always
fit in a single datagram. An example is name lookup. When a user attempts to
make a connection to another system, he will generally specify the system by
name, rather than Internet address. His system has to translate that name to
an address before it can do anything. Generally, only a few systems have the
database used to translate names to addresses. So the user's system will want
to send a query to one of the systems that has the database.

This query is going to be very short. It will certainly fit in one datagram.
So will the answer. Thus it seems silly to use TCP. Of course TCP does more
than just break things up into datagrams. It also makes sure that the data
arrives, resending datagrams where necessary. But for a question that fits in
a single datagram, all of the complexity of TCP is not needed. If there is not
an answer after a few seconds, you can just ask again. For applications like
this, there are alternatives to TCP.

The most common alternative is UDP ("user datagram protocol"). UDP is designed
for applications where you don't need to put sequences of datagrams together.
It fits into the system much like TCP. There is a UDP header. The network
software puts the UDP header on the front of your data, just as it would put a
TCP header on the front of your data. Then UDP sends the data to IP, which
adds the IP header, putting UDP's protocol number in the protocol field instead
of TCP's protocol number.

UDP doesn't do as much as TCP does. It does not split data into multiple
datagrams and it does not keep track of what it has sent so it can resend if
necessary. About all that UDP provides is port numbers so that several
programs can use UDP at once. UDP port numbers are used just like TCP port
numbers. There are well-known port numbers for servers that use UDP.

The UDP header is shorter than a TCP header. It still has source and
destination port numbers, and a checksum, but that's about it. UDP is used by
the protocols that handle name lookups (see IEN 116, RFC 882, and RFC 883) and
a number of similar protocols.

Another alternative protocol is ICMP ("Internet control message protocol").
ICMP is used for error messages, and other messages intended for the TCP/IP
software itself, rather than any particular user program. For example, if you
attempt to connect to a host, your system may get back an ICMP message saying
"host unreachable." ICMP can also be used to find out some information about
the network. See RFC 792 for details of ICMP.

ICMP is similar to UDP, in that it handles messages that fit in one datagram.
However it is even simpler than UDP. It does not even have port numbers in its
header. Since all ICMP messages are interpreted by the network software
itself, no port numbers are needed to say where an ICMP message is supposed to
go.

Keeping Track Of Names And Information: The Domain System
~~~~~~
As we indicated earlier, the network software generally needs a 32-bit Internet
address in order to open a connection or send a datagram. However users prefer
to deal with computer names rather than numbers. Thus there is a database that
allows the software to look up a name and find the corresponding number.

When the Internet was small, this was easy. Each system would have a file that
listed all of the other systems, giving both their name and number. There are
now too many computers for this approach to be practical. Thus these files

have been replaced by a set of name servers that keep track of host names and the corresponding Internet addresses. (In fact these servers are somewhat more general than that. This is just one kind of information stored in the domain system.) A set of interlocking servers are used rather than a single central one.

There are now so many different institutions connected to the Internet that it would be impractical for them to notify a central authority whenever they installed or moved a computer. Thus naming authority is delegated to individual institutions. The name servers form a tree, corresponding to institutional structure. The names themselves follow a similar structure. A typical example is the name BORAX.LCS.MIT.EDU. This is a computer at the Laboratory for Computer Science (LCS) at MIT. In order to find its Internet address, you might potentially have to consult 4 different servers.

First, you would ask a central server (called the root) where the EDU server is. EDU is a server that keeps track of educational institutions. The root server would give you the names and Internet addresses of several servers for EDU. You would then ask EDU where the server for MIT is. It would give you names and Internet addresses of several servers for MIT. Then you would ask MIT where the server for LCS is, and finally you would ask one of the LCS servers about BORAX. The final result would be the Internet address for BORAX.LCS.MIT.EDU. Each of these levels is referred to as a "domain." The entire name, BORAX.LCS.MIT.EDU, is called a "domain name." (So are the names of the higher-level domains, such as LCS.MIT.EDU, MIT.EDU, and EDU.)

Fortunately, you don't really have to go through all of this most of the time. First of all, the root name servers also happen to be the name servers for the top-level domains such as EDU. Thus a single query to a root server will get you to MIT. Second, software generally remembers answers that it got before. So once we look up a name at LCS.MIT.EDU, our software remembers where to find servers for LCS.MIT.EDU, MIT.EDU, and EDU. It also remembers the translation of BORAX.LCS.MIT.EDU. Each of these pieces of information has a "time to live" associated with it. Typically this is a few days. After that, the information expires and has to be looked up again. This allows institutions to change things.

The domain system is not limited to finding out Internet addresses. Each domain name is a node in a database. The node can have records that define a number of different properties. Examples are Internet address, computer type, and a list of services provided by a computer. A program can ask for a specific piece of information, or all information about a given name. It is possible for a node in the database to be marked as an "alias" (or nickname) for another node. It is also possible to use the domain system to store information about users, mailing lists, or other objects.

There is an Internet standard defining the operation of these databases as well as the protocols used to make queries of them. Every network utility has to be able to make such queries since this is now the official way to evaluate host names. Generally utilities will talk to a server on their own system. This server will take care of contacting the other servers for them. This keeps down the amount of code that has to be in each application program.

The domain system is particularly important for handling computer mail. There are entry types to define what computer handles mail for a given name to specify where an individual is to receive mail and to define mailing lists.

See RFCs 882, 883, and 973 for specifications of the domain system. RFC 974 defines the use of the domain system in sending mail.

Routing
~~~~~~~
The task of finding how to get a datagram to its destination is referred to as "routing." Many of the details depend upon the particular implementation. However some general things can be said.

It is necessary to understand the model on which IP is based. IP assumes that a system is attached to some local network. It is assumed that the system can send datagrams to any other system on its own network. (In the case of Ethernet, it simply finds the Ethernet address of the destination system, and

puts the datagram out on the Ethernet.) The problem comes when a system is
asked to send a datagram to a system on a different network. This problem is
handled by gateways.

A gateway is a system that connects a network with one or more other networks.
Gateways are often normal computers that happen to have more than one network
interface. The software on a machine must be set up so that it will forward
datagrams from one network to the other. That is, if a machine on network
128.6.4 sends a datagram to the gateway, and the datagram is addressed to a
machine on network 128.6.3, the gateway will forward the datagram to the
destination. Major communications centers often have gateways that connect a
number of different networks.

Routing in IP is based entirely upon the network number of the destination
address. Each computer has a table of network numbers. For each network
number, a gateway is listed. This is the gateway to be used to get to that
network. The gateway does not have to connect directly to the network, it just
has to be the best place to go to get there.

When a computer wants to send a datagram, it first checks to see if the
destination address is on the system's own local network. If so, the datagram
can be sent directly. Otherwise, the system expects to find an entry for the
network that the destination address is on. The datagram is sent to the
gateway listed in that entry. This table can get quite big. For example, the
Internet now includes several hundred individual networks. Thus various
strategies have been developed to reduce the size of the routing table. One
strategy is to depend upon "default routes." There is often only one gateway
out of a network.

This gateway might connect a local Ethernet to a campus-wide backbone network.
In that case, it is not neccessary to have a separate entry for every network
in the world. That gateway is simply defined as a "default." When no specific
route is found for a datagram, the datagram is sent to the default gateway. A
default gateway can even be used when there are several gateways on a network.
There are provisions for gateways to send a message saying "I'm not the best
gateway -- use this one instead." (The message is sent via ICMP. See RFC
792.) Most network software is designed to use these messages to add entries
to their routing tables. Suppose network 128.6.4 has two gateways, 128.6.4.59
and 128.6.4.1. 128.6.4.59 leads to several other internal Rutgers networks.
128.6.4.1 leads indirectly to the NSFnet. Suppose 128.6.4.59 is set as a
default gateway, and there are no other routing table entries. Now what
happens when you need to send a datagram to MIT? MIT is network 18. Since
there is no entry for network 18, the datagram will be sent to the default,
128.6.4.59. This gateway is the wrong one. So it will forward the datagram to
128.6.4.1. It will also send back an error saying in effect: "to get to
network 18, use 128.6.4.1." The software will then add an entry to the routing
table. Any future datagrams to MIT will then go directly to 128.6.4.1. (The
error message is sent using the ICMP protocol. The message type is called
"ICMP redirect.")

Most IP experts recommend that individual computers should not try to keep
track of the entire network. Instead, they should start with default gateways
and let the gateways tell them the routes as just described. However this
doesn't say how the gateways should find out about the routes. The gateways
can't depend upon this strategy. They have to have fairly complete routing
tables. For this, some sort of routing protocol is needed. A routing protocol
is simply a technique for the gateways to find each other and keep up to date
about the best way to get to every network. RFC 1009 contains a review of
gateway design and routing.

Details About Internet Addresses: Subnets And Broadcasting
~~~~~~
Internet addresses are 32-bit numbers, normally written as 4 octets (in
decimal), e.g. 128.6.4.7. There are actually 3 different types of address.
The problem is that the address has to indicate both the network and the host
within the network. It was felt that eventually there would be lots of
networks. Many of them would be small, but probably 24 bits would be needed to
represent all the IP networks. It was also felt that some very big networks
might need 24 bits to represent all of their hosts. This would seem to lead to

48 bit addresses. But the designers really wanted to use 32 bit addresses. So
they adopted a kludge. The assumption is that most of the networks will be
small. So they set up three different ranges of address.

Addresses beginning with 1 to 126 use only the first octet for the network
number. The other three octets are available for the host number. Thus 24
bits are available for hosts. These numbers are used for large networks, but
there can only be 126 of these. The ARPAnet is one and there are a few large
commercial networks. But few normal organizations get one of these "class A"
addresses.

For normal large organizations, "class B" addresses are used. Class B
addresses use the first two octets for the network number. Thus network
numbers are 128.1 through 191.254. (0 and 255 are avoided for reasons to be
explained below. Addresses beginning with 127 are also avoided because they
are used by some systems for special purposes.) The last two octets are
available for host addesses, giving 16 bits of host address. This allows for
64516 computers, which should be enough for most organizations. Finally, class
C addresses use three octets in the range 192.1.1 to 223.254.254. These allow
only 254 hosts on each network, but there can be lots of these networks.
Addresses above 223 are reserved for future use as class D and E (which are
currently not defined).

0 and 255 have special meanings. 0 is reserved for machines that do not know
their address. In certain circumstances it is possible for a machine not to
know the number of the network it is on, or even its own host address. For
example, 0.0.0.23 would be a machine that knew it was host number 23, but
didn't know on what network.

255 is used for "broadcast." A broadcast is a message that you want every
system on the network to see. Broadcasts are used in some situations where you
don't know who to talk to. For example, suppose you need to look up a host
name and get its Internet address. Sometimes you don't know the address of the
nearest name server. In that case, you might send the request as a broadcast.
There are also cases where a number of systems are interested in information.
It is then less expensive to send a single broadcast than to send datagrams
individually to each host that is interested in the information. In order to
send a broadcast, you use an address that is made by using your network
address, with all ones in the part of the address where the host number goes.
For example, if you are on network 128.6.4, you would use 128.6.4.255 for
broadcasts. How this is actually implemented depends upon the medium. It is
not possible to send broadcasts on the ARPAnet, or on point to point lines, but
it is possible on an Ethernet. If you use an Ethernet address with all its
bits on (all ones), every machine on the Ethernet is supposed to look at that
datagram.

Because 0 and 255 are used for unknown and broadcast addresses, normal hosts
should never be given addresses containing 0 or 255. Addresses should never
begin with 0, 127, or any number above 223.

Datagram Fragmentation And Reassembly
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
TCP/IP is designed for use with many different kinds of networks.
Unfortunately, network designers do not agree about how big packets can be.
Ethernet packets can be 1500 octets long. ARPAnet packets have a maximum of
around 1000 octets. Some very fast networks have much larger packet sizes.
You might think that IP should simply settle on the smallest possible size, but
this would cause serious performance problems. When transferring large files,
big packets are far more efficient than small ones. So it is best to be able
to use the largest packet size possible, but it is also necessary to be able to
handle networks with small limits. There are two provisions for this.

TCP has the ability to "negotiate" about datagram size. When a TCP connection
first opens, both ends can send the maximum datagram size they can handle. The
smaller of these numbers is used for the rest of the connection. This allows
two implementations that can handle big datagrams to use them, but also lets
them talk to implementations that cannot handle them. This does not completely
solve the problem. The most serious problem is that the two ends do not
necessarily know about all of the steps in between. For this reason, there are

provisions to split datagrams up into pieces. This is referred to as
"fragmentation."

The IP header contains fields indicating that a datagram has been split and
enough information to let the pieces be put back together. If a gateway
connects an Ethernet to the Arpanet, it must be prepared to take 1500-octet
Ethernet packets and split them into pieces that will fit on the Arpanet.
Furthermore, every host implementation of TCP/IP must be prepared to accept
pieces and put them back together. This is referred to as "reassembly."

TCP/IP implementations differ in the approach they take to deciding on datagram
size. It is fairly common for implementations to use 576-byte datagrams
whenever they can't verify that the entire path is able to handle larger
packets. This rather conservative strategy is used because of the number of
implementations with bugs in the code to reassemble fragments. Implementors
often try to avoid ever having fragmentation occur. Different implementors
take different approaches to deciding when it is safe to use large datagrams.
Some use them only for the local network. Others will use them for any network
on the same campus. 576 bytes is a "safe" size which every implementation must
support.

Ethernet Encapsulation: ARP
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
In Part One of Introduction to the Internet Protocols (Phrack Inc., Volume
Three, Issue 28, File #3 of 12) there was a brief description about what IP
datagrams look like on an Ethernet. The discription showed the Ethernet header
and checksum, but it left one hole: It did not say how to figure out what
Ethernet address to use when you want to talk to a given Internet address.
There is a separate protocol for this called ARP ("address resolution
protocol") and it is not an IP protocal as ARP datagrams do not have IP
headers.

Suppose you are on system 128.6.4.194 and you want to connect to system
128.6.4.7. Your system will first verify that 128.6.4.7 is on the same
network, so it can talk directly via Ethernet. Then it will look up 128.6.4.7
in its ARP table to see if it already knows the Ethernet address. If so, it
will stick on an Ethernet header and send the packet. Now suppose this system
is not in the ARP table. There is no way to send the packet because you need
the Ethernet address. So it uses the ARP protocol to send an ARP request.
Essentially an ARP request says "I need the Ethernet address for 128.6.4.7".
Every system listens to ARP requests. When a system sees an ARP request for
itself, it is required to respond. So 128.6.4.7 will see the request and will
respond with an ARP reply saying in effect "128.6.4.7 is 8:0:20:1:56:34". Your
system will save this information in its ARP table so future packets will go
directly.

ARP requests must be sent as "broadcasts." There is no way that an ARP request
can be sent directly to the right system because the whole reason for sending
an ARP request is that you do not know the Ethernet address. So an Ethernet
address of all ones is used, i.e. ff:ff:ff:ff:ff:ff. By convention, every
machine on the Ethernet is required to pay attention to packets with this as an
address. So every system sees every ARP requests. They all look to see
whether the request is for their own address. If so, they respond. If not,
they could just ignore it, although some hosts will use ARP requests to update
their knowledge about other hosts on the network, even if the request is not
for them. Packets whose IP address indicates broadcast (e.g. 255.255.255.255
or 128.6.4.255) are also sent with an Ethernet address that is all ones.

Getting More Information
~~~~~~~~~~~~~~~~~~~~~~~~~~
This directory contains documents describing the major protocols. There are
hundreds of documents, so I have chosen the ones that seem most important.
Internet standards are called RFCs (Request for Comments). A proposed standard
is initially issued as a proposal, and given an RFC number. When it is finally
accepted, it is added to Official Internet Protocols, but it is still referred
to by the RFC number. I have also included two IENs (Internet Engineering
Notes). IENs used to be a separate classification for more informal
documents, but this classification no longer exists and RFCs are now used for
all official Internet documents with a mailing list being used for more

informal reports.

The convention is that whenever an RFC is revised, the revised version gets a
new number. This is fine for most purposes, but it causes problems with two
documents: Assigned Numbers and Official Internet Protocols. These documents
are being revised all the time and the RFC number keeps changing. You will
have to look in rfc-index.txt to find the number of the latest edition. Anyone
who is seriously interested in TCP/IP should read the RFC describing IP (791).
RFC 1009 is also useful as it is a specification for gateways to be used by
NSFnet and it contains an overview of a lot of the TCP/IP technology.

Here is a list of the documents you might want:

```
    rfc-index List of all RFCs
    rfc1012   Somewhat fuller list of all RFCs
    rfc1011   Official Protocols.  It's useful to scan this to see what tasks
              protocols have been built for.  This defines which RFCs are
              actual standards, as opposed to requests for comments.
    rfc1010   Assigned Numbers.  If you are working with TCP/IP, you will
              probably want a hardcopy of this as a reference.  It lists all
              the offically defined well-known ports and lots of other
              things.
    rfc1009   NSFnet gateway specifications.  A good overview of IP routing
              and gateway technology.
    rfc1001/2 NetBIOS:  Networking for PCs
    rfc973    Update on domains
    rfc959    FTP (file transfer)
    rfc950    Subnets
    rfc937    POP2:  Protocol for reading mail on PCs
    rfc894    How IP is to be put on Ethernet, see also rfc825
    rfc882/3  Domains (the database used to go from host names to Internet
              address and back -- also used to handle UUCP these days).  See
              also rfc973
    rfc854/5  Telnet - Protocol for remote logins
    rfc826    ARP - Protocol for finding out Ethernet addresses
    rfc821/2  Mail
    rfc814    Names and ports - General concepts behind well-known ports
    rfc793    TCP
    rfc792    ICMP
    rfc791    IP
    rfc768    UDP
    rip.doc   Details of the most commonly-used routing protocol
    ien-116   Old name server (still needed by several kinds of systems)
    ien-48    The Catenet model, general description of the philosophy behind
              TCP/IP
```

The following documents are somewhat more specialized.

```
    rfc813    Window and acknowledgement strategies in TCP
    rfc815    Datagram reassembly techniques
    rfc816    Fault isolation and resolution techniques
    rfc817    Modularity and efficiency in implementation
    rfc879    The maximum segment size option in TCP
    rfc896    Congestion control
    rfc827,888,904,975,985    EGP and related issues
```

The most important RFCs have been collected into a three-volume set, the DDN
Protocol Handbook. It is available from the DDN Network Information Center at
SRI International. You should be able to get them via anonymous FTP from
SRI-NIC.ARPA. The file names are:

```
  RFCs:
    rfc:rfc-index.txt
    rfc:rfcxxx.txt
  IENs:
    ien:ien-index.txt
    ien:ien-xxx.txt
```

 Sites with access to UUCP, but not FTP may be able to retreive them via
 UUCP from UUCP host rutgers. The file names would be

```
RFCs:
   /topaz/pub/pub/tcp-ip-docs/rfc-index.txt
   /topaz/pub/pub/tcp-ip-docs/rfcxxx.txt
IENs:
   /topaz/pub/pub/tcp-ip-docs/ien-index.txt
   /topaz/pub/pub/tcp-ip-docs/ien-xxx.txt

                >-------=====END=====-------<
```

==Phrack Inc.==

Volume Three, Issue 29, File #4 of 12

Network Miscellany II
~~~~~~~~~~~~~~~~~~~~~~
by Taran King

November 17, 1989

BROADCASTING NETWORKS
~~~~~~~~~~~~~~~~~~~~~~~
Although these articles discuss things about communicating through computer
networks, there are ways to contact broadcasting networks via the nets. The
Public Broadcasting Service (PBS) has their own UUCP node:

Public Broadcasting Service (PBS)
UUCP Node name: pbs
Node contact: pbs!postmaster (Senton R. Droppers)
Telephone number: (703) 739-5089

There are also a number of radio stations that can be contacted via Fidonet:

KFCF
Fresno, CA
Contact: Randy.Stover@f42.n205.z1.fidonet.org

KKSF
San Fransisco, CA
Contact: Tim.Pozar@fidogate.fidonet.org

KKDA
Dallas, TX
Contact: Gerry.Dalton@f1213.n124.z1.fidonet.org

ECNCDC (BITNET)
~~~~~~~~~~~~~~~~
Western Illinois University, Eastern Illinois University as well as the
University of Northeastern Illinois, Chicago State University and Governors
State University are part of the Educational Computing Network. The
Educational Computing Network is a service of the Board of Governors of State
Colleges and Universities operating as a cooperative to supply mainframe
academic computing resources to each of its members (ECN is strictly for
academic use and does no administrative computing). The cooperative effort of
the members of the Educational Computing Network allows for more academic
computing resources to be made available to the members than they could supply
on their own.

Each member institution of the Educational Computing Network has a unique
letter for the first letter in all their user names. The letters are:

     Chicago State University   - B
     Eastern Illinois University   - C
     Governors State University   - G
     Western Illinois University   - M
     University of Northeastern Illinois - U

Each member of ECN also has a person which is the interface between ECN and the
university called their User Coordinator. The User Coordinator's username
consists of their school letter followed by UCM000 (the User Coordinator for
WIU is MUCM000).

For more information about the Educational Computing Network, contact
XJJGUDE@ECNCDC.BITNET

MCI MAIL
~~~~~~~~

If you read the first Network Miscellany article which appeared in Phrack 28,
you may remember my mentioning CMR, the Commercial Mail Relay. Unfortunately,
due to its restrictions about who can use it (supposedly), it has potential to
become a sticky situation if the user you are sending to no longer has his MCI
Mail account or if you accidentally mistype the MCI Mail address. But to save
us from this potential problem, MCI Mail now has their own domain on the
Internet, MCIMAIL.COM so mailing to userid@MCIMAIL.COM should work just as well
as CMR without the risks of being yelled at (and possibly billed).

PUBLIC ACCESS UNIXES
~~~~~~~~~~~~~~~~~~~~~~
Part of the problem with the whole idea of using the Wide Area Networks is
access. For those who are not enrolled in a university or cannot pull strings
at their local business or college, the concept of communicating through the
networks is useless besides thinking that it would be neat. Thanks to Phil
Eschallier, phil@lgnp1.UUCP or phil@LS.COM, you should now be able to get
access to the Wide Area Networks via UUCP. The following is a list of Public
Access Unix systems taken from the Usenet Newsgroup pub.nixpub which Phil keeps
up and there are two versions, both of which contain the same basic information
but each has important information which the other does not necessarily have.
I urge you to attempt to get on one of these systems and drop us a line over
the networks.

                       nixpub long listing
        Open Access UNIX (*NIX) Sites [Fee / No Fee] for mapped sites only
                       [November 12, 1989]

Systems listed (73):
  [agora, alphacm, althea, amazing, anet, attctc, bigtex, bucket, chariot]
  [chinet, cinnet, conexch, cpro, cruzio, dasys1, ddsw1, dhw68k, disk   ]
  [eklektik, esfenn, gensis, grebyn, i-core, igloo, jdyx, jolnet, lgnp1   ]
  [lilink, loft386, lunapark, m-net, madnix, magpie, marob, ncoast, netcom]
  [nstar, nuchat, nucleus, oncoast, ozdaltx, pallas, pnet01, pnet02   ]
  [pnet51, point, polari, portal, raider, rpp386, rtmvax, sactoh0, sharks]
  [sir-alan, sixhub, stanton, stb, sugar, telly, tmsoft, tnl, turnkey   ]
  [ubbs-nh, usource, uuwest, vpnet, well, wet, wolves, world, wybbs   ]
  [xroads, ziebmef   ]

Last
Contact
Date   Telephone #   Sys-name   Location   Baud   Hours
-----   ------------   --------   -----------   -------   -----

08/89 201-846-2460^ althea   New Brunswick   NJ 3/12/24   24
   AT&T 3B2/310 - Unix SVR3.1, no fee. USENET, email, C development,
   games. Single line.
   Contact: rjd@althea.UUCP (Robert Diamond)

10/89 206-328-4944   polari   Seattle   WA 3/12   24
   Equip ???; 8-lines, Trailblazer on 206-328-1468; $30/year (flat rate);
   Multi-user games, chat, full USENET.
   Contact: uunet!microsoft!happym!polari!bruceki

10/89 212-420-0527   magpie   NYC   NY 3/12/24/96 24
   ? - UNIX SYSV - 2, Magpie BBS, no fee, Authors: Magpie/UNIX,/MSDOS
   two lines plus anonymous uucp: 212-677-9487 (9600 bps Telebit modem)
   NOTE: 9487 reserved for registered Magpie sysops & anon uucp
   Contact: Steve Manes, {rutgers|cmcl2|uunet}!hombre!magpie!manes

10/89 212-675-7059   marob   NYC   NY 3/12/24   24
   386 SCO-XENIX 2.2, XBBS, magpie bbs, no fee, limit 60 min
   Telebit Trailblazer (9600 PEP) only 212-675-8438
   Contact: {philabs|rutgers|cmcl2}!{phri|hombre}!marob!clifford

05/89 212-879-9031^ dasys1   NYC   NY 12/24   24
   Unistride - SYS V, multiple lines, fee $5/mo AKA Big Electric Cat
   USENET, games, multi-user chat, email, login: new, passwd: new
   Contact: ...!rutgers!cmcl2!rsweeney or rsweeney@dasys1.UUCP

```
09/89  213-376-5714^  pnet02     Redondo Bch      CA  3/12/24       24
   XENIX (also 213-374-7404) no fee, 90 min limit, login: pnet id: new
   some USENET, net-work e-mail, multi-threaded conferencing

09/89  213-397-3137^  stb        Santa Monica     CA  3/12/24       24
   AT&T 3b1;  BBS and shell access;  uucp-anon: ogin: uucp NO PASSWD
   3 line on rotory -3137 2400 baud.

03/88  213-459-5891   amazing    Pacific Palisades CA  3/12/24       24
   AMT 286 - Microport  David's Amazing BBS  Fee $7.50/month;$35/6;$60/year
   5 lines on rotary; Unique original software with conferencing, electronic
   bar, matchmaking, no file up/downloading

07/88  214-247-2367   ozdaltx    Dallas           TX  3/12/24       24
   INTEC/SCO XENIX 2.2.1, OZ BBS, Membership only adult BBS, fee $40
   year. Multiple lines.  Closed system, carries limited USENET
   newsgroups. Login: guest (no PW).  Voice verification on all new users.

07/89  214-824-7881   attctc     Dallas           TX  3/12/24       24
   3b2/522 - UNIX, no fee, various time limits, 8 lines 2.8 GB online
   uucp-anon --> 214-741-2130  ogin: uupdsrc word: Public
   uucp-anon info in: /bbsys4/README     (Formerly node name killer)

11/89  215-348-9727   lgnp1      Doylestown       PA  3/12/24/96  24
   SCO-XENIX -- Telebit access.  Shell accounts by appointment only;  Fee;
   Services include E-mail, USENET News;  --Home of the Nixpub lists--
   Contact: phil@ls.com.
     anon-uucp: nuucp  NO PWD  (download /usr/spool/uucppublic/nixpub
                                 or /usr/spool/uucppublic/nixpub.short)

09/89  216-582-2441   ncoast     Cleveland        OH  12/24/96      24
   80386 Mylex, SCO Xenix;  600 meg. storage;  XBBS and Shell;  USENET
   (newsfeeds available), E-Mail; donations requested; login as "bbs"
   for BBS and "makeuser" for new users.
   Telebit used on 216-237-5486.

08/88  217-529-3223   pallas     Springfield      IL  3/12/24       24
   Convrgnt Minifrme, multiple lines, 200 meg Minnie bbs $25 donation

10/89  219-289-0286   nstar      South Bend       IN  3/12/24/96  24
   Equip ???, UNIX 3.2; 300 Meg On-line; 4 lines at 9600 baud --
   (listed) - Hayes V-Series, (287-9020) - HST, (289-3745) - PEP;
   Full USENET, AKCS Software; Contact ..!iuvax!ndcheg!ndmath!nstar!larry

08/88  312-283-0559^  chinet     Chicago          IL  3/12/24       24
   3b2/300 - SYS V 3.1, multiple lines, Picospan BBS, system & BBS free
   Extra phone lines and usenet, $50/yr.

10/89  312-338-0632^  point      Chicago          IL  3/12/24/96  24
   North Shore / Rogers Park area of Chicago.  386 - ISC 2.01 (SysV3.2),
   multiple lines, Telebit PEP on 338-3261, USRobotics HST on 338-1036,
   AKCS bbs, some usenet conferences available.  200+ MB online storage.
   Downloads, full usenet & shell access in the works.

04/89  313-623-6309   nucleus    Clarkston        MI  12/24        24
   286 - Unix System V, no fee. Shell access, full usenet access, online games,
   AKCS conferencing system, some public domain sources online, extensive tape
   library of public domain source code

02/88  313-994-6333   m-net      Ann Arbor        MI  3/12         24
   Altos 68020 - SYS III, limits unstated, fee for extended service
   Picospan conference system, multiple lines, 160 meg, packet radio

08/89  313-996-4644^  anet       Ann Arbor        MI  3/12         24
   Altos 68000 - Sys III, no limits, 1st month free, fees range up to $20/
   month (negotiable), accepts equipment/software in lieu of fees, Picospan
   conferencing, 120M, non-profit, user-supported, community-based, ideal
   autodidact educational system.  Tax-deductible donations okay.

08/89  314-474-4581   gensis     Columbia         MO  3/12/24/48/96  24
```

Gateway 386 system w/ SCO Xenix V/386, DataFlex, Oracle, CHARM, & VP/ix.
No fee. Online gaming, game design, and (oddly enough) data base design
are the main focus. Modem is Microcom MNP 6.

10/89 404-321-5020^ jdyx   Atlanta   GA 12/24/96   24
  386/ix 2.0.2. XBBS. Usenet (alt, gnu, most comp and a few others) and
  shell access. Second line (2400 below) (404) 325-1719. 200+ meg current
  Usenet and GNU sources. Specializing in graphics and ray-tracing under
  386/ix (with/with out X11). Yearly fee for shell and/or downloads.
  Telebit access. Contact: ...gatech!emory!jdyx!tpf (Tom Friedel)

05/88 407-380-6228 rtmvax   Orlando   FL 3/12/24   24
  mVAX-I - Ultrix-32 V1.2 USENET & UUCP Email Gateway. XBBS front end for
  new user subscribing. No Fees. Primary function is Technical exchange.
  Contact: { cbosgd!codas, hoptoad!peora }!rtmvax!rob

09/89 408-245-7726^ uuwest   Sunnyvale   CA 3/12/24   24
  SCO-XENIX, Waffle. No fee, USENET news (news.*, music, comics, telecom, etc)
  The Dark Side of the Moon BBS. This system has been in operation since 1985.
  Login: new Contact: (UUCP) ames!uuwest!request (Domain) request@darkside.com

04/88 408-247-4810 sharks   Santa Clara   CA 3/12   24
  Altos 886/80/80 - XENIX 3.2f AKA: Shark's Head BBS, BBCS Network
  Multiple lines,no fee for non-members,members $25 year
  Restricted sh access and UUCP/Usenet access for advanced members

11/89 408-423-9995 cruzio   Santa Cruz   CA 12/24   24
  Tandy 4000, Xenix 2.3.*, Caucus 3.*; focus on Santa Cruz activity
  (ie directory of community and goverment organizations, events, ...);
  Multiple lines; no shell; fee: $18/quarter.
  Contact: ...!uunet!cruzio!chris

10/89 408-725-0561^ portal   Cupertino   CA 3/12/24   24
  Networked Suns (SunOS), multiple lines, Telenet access, no shell access
  fees: $10/month + Telenet charges (if used) @ various rates/times
  conferencing, multi user chats, usenet

02/89 408-997-9119^ netcom   San Jose   CA 3/12/24/96 24
  Unix System V -- Shell Access [Bourne, Korn, C-Shell], BBS, USENET,
  Languages: C, Lisp, Prolog, Clips, (Ada soon), $10 / month, login as
  'guest' no password. Contact netcom!bobr.

10/89 412-431-8649 eklektik   Pittsburgh   PA 3/12/24   24
  UNIX PC- SYSV - UNaXcess BBS, new system - donation requested for shell,
  login: bbs for BBS, uucp-mail, limited Usenet news feeds. Gaming SIGS.
  Contact: ...!gatech!emoryu1!eklektik!anthony

11/89 415-332-6106^ well   Sausalito   CA 12/24   24
  6-processor Sequent Balance (32032); UUCP and USENET access; multiple
  lines; access via CPN; PICOSPAN BBS; $3/hour. Contact (415) 332-4335

06/88 415-582-7691 cpro   Hayward   CA 12/24   24
  Microport SYSV 2, UNaXcess bbs, no fee, 60 min limit, shell access

07/89 415-753-5265^ wet   San Francisco   CA 3/12/24   24
  386 SYS V.3. Wetware Diversions. $15 registration, $0.01/minute.
  Public Access UNIX System: uucp, PicoSpan bbs, full Usenet News,
  multiple lines, shell access. Newusers get initial credit!
  contact:{ucsfcca|claris|hoptoad}!wet!cc (Christopher Cilley)

05/89 415-783-2543 esfenn   Hayward   CA 3/12/24   24
  System ????; USENET news; E-mail; No charges; Contact esfenn!william.

01/89 416-452-0926 telly   Brampton   ON 12/24/96   24
  286 Xenix; proprietary menu-based BBS includes Usenet site searching.
  News (all groups, incl biz, pubnet, gnu), mail (including to/from Internet),
  some archives. Feeds available. Fee: $75(Cdn)/year.
  Contact: Evan Leibovitch, evan@telly.on.ca, {uunet!attcan,utzoo}!telly!evan

12/88 416-461-2608 tmsoft   Toronto   ON 3/12/24/96 24

     NS32016, Sys5r2, shell; news+mail $30/mo, general-timesharing $60/mo
     All newsgroups. Willing to setup mail/news connections.
     Archives:comp.sources.{unix,games,x,misc}
     Contact: Dave Mason <mason@tmsoft> / Login: newuser

07/89 416-654-8854   ziebmef   Toronto   ON 3/12/24/96 24
     AT&T 3B1, Sys V, shell, news, mail, no fee (donations accepted)
     Carries most newsgroups (willing to add extra ones on request)
     Telebit access, willing to give mail feeds
     Contact: Chris Siebenmann, {utzoo!telly,ncrcan}!ziebmef!cks

08/89 502-968-5401   disk   Louisville   KY 3/12   24
     386 clone, Microport System V, 600 meg. 6 lines 5401 thru 5406.
     rarrying most USENET groups, Shell access, games, downloads,
     multi-user chat, and more. Rate info available via a free trial
     account.

12/88 503-254-0458   bucket   Portland   OR 3/12/24   24
     Tektronix 6130, UTek 2.3(4.2BSD-derived). Bit Bucket BBS publically
     available; login as 'bbs'. BBS is message only. Users intereseted in
     access to Unix should contact SYSOP via the BBS or send EMail to
     ..tektronix!tessi!bucket!rickb. Unix services include USENET News,
     EMail, and all tools/games/utility access. Alternate dial-in lines
     available for Unix users.

05/89 503-640-4262^ agora   PDX   OR 3/12/24   24
     Intel Xenix-286, $2/mo or $20/yr, news, mail, games, programming
     two lines with trunk-hunt, 4380 supports MNP level 3.
     Contact: Alan Batie, tektronix!tessi!agora!batie

10/89 512-346-2339   bigtex   Austin   TX 96   24
     Equip unknown, no shell, no fee, anonymous uucp ONLY, Telebit 9600/PEP
     mail & newsfeeds (limited) available. Carries GNU software.
     anon login: nuucp NO PASSWD, file list /usr3/index
     Contact: ...!uunet!utastro!bigtex!james

07/89 512-832-8835   rpp386   Austin   TX 12/24   24
     386 SYSV, no shell, no bbs, anonymous uucp file transfer site only, no fee
     uucp and kermit server available, login uucp or kermit NO PASSWD

10/89 513-779-8209   cinnet   Cincinnati   OH 12/24/96   24
     80386, ISC 386/ix 2.02, Telebit access, 1 line; $7.50/Month; shell
     access, Usenet access; news feeds available;
     login: newact password: new user to register for shell access

05/89 516-872-2137   lilink   Long Island   NY 12/24   24
     80386/20 Mhz. , three lines, News/Mail/Shell access. Online games,
     conferencing, full program development system, full text processing.
     We carry ALL Usenet groups. Dues are $10/month (unlimited access).
     Accounts are filled by application/phone verification. Login: new
     Alternate numbers: 516-872-2138 & 516-872-2349

07/89 517-487-3356   lunapark   E. Lansing   MI 12/24   24
     Compaq 386/20 SCO-XENIX 2.3.1, lunabbs bulletin board & conferencing
     system, no fee, login: bbs no password. Primarily UNIX software
     with focus on TeX and Postscript, also some ATARI-ST and IBM-PC stuff
     2400/1200 --> 8 N 1
     Contact: ...!uunet!frith!lunapark!larry

12/88 518-346-8033   sixhub   upstate   NY 3/12/24   24
     PC Designs GV386. hub machine of the upstate NY UNIX users group (*IX)
     two line reserved for incoming, bbs no fee, news & email fee $15/year
     Smorgasboard of BBS systems, UNaXcess and XBBS online,
     Citadel BBS now in production. Contact: davidsen@sixhub.uucp.

09/88 602-941-2005   xroads   Phoenix   AZ 12/24   24
     Motorola VME1121, UNIX 5.2, Crossroads BBS, Fee $30/yr + $.50/.25 (call)
     prime (evenings)/non-prime, USENET news, multi-chat, online games,
     movie reviews, adventure games, dos unix/xenix files for dload, multi lines

```
08/89  603-880-8120  ubbs-nh    Nashua          NH 3/12/24/96  24
  New England Unix Archive Site.  Multiple lines.  Services include E-Mail,
  full or partial news feeds.  XBBS access $25/year, User Accounts or News
  Feeds available $60/year (1 hour/day) or $120/year (2 hours/day).
  Contact:  noel@ubbs-nh or {decvax}!ubbs-nh!noel or leave message on the
  bbs.  Voice:  603 595-2947

08/89  605-348-2738  loft386    Rapid City      SD 3/12/24/96  24
  80386 SYS V/386 Rel 3.2, Usenet mail/news via UUNET, UUNET archive access.
  NO BBS!  News feeds avaliable.  400 meg hd.  Fees: $10/month or $25/quarter.
  Call (605) 343-8760 and talk to Doug Ingraham to arrange an account or email
  uunet!loft386!dpi

08/88  608-273-2657  madnix     Madison         WI 3/12/24    24
  286 SCO-XENIX, shell, no fee, USENET news, mail, login: newuser
  Contact: ray@madnix

08/89  612-473-2295  pnet51     Minneapolis     MN 3/12/24    24
  Equip ?, Xenix, multi-line, no fee, some Usenet news, email, multi-threaded
  conferencing, login: pnet id: new, PC Pursuitable
  UUCP: {rosevax, crash}!orbit!pnet51!admin

08/89  615-896-8716  raider     Murfreesboro    TN 12/24      24
  Tandy 4000 XENIX, XBBS, shell accounts, news and mail, newsfeeds
  available. Two line system; second dialup is 615-896-7905.
  Contact: root@raider.MFEE.TN.US (Bob Reineri); NO CHARGE.

07/89  616-457-1964  wybbs      Jenison         MI 3/12/24    24
  286 - SCO-XENIX 2.2.1, no fees, two lines, shell access, usenet news,
  150 meg storage, XBBS, interests: ham radio, xenix
  AKA: Consultants Connection  Contact: danielw@wybbs.UUCP
  Alternate phone #: 616-457-9909 (max 1200 baud)

11/89  617-739-9753  world      Brookline       MA 3/12/24/96  24
  Sun 4/280, SunOS 4.03;  Shell, USENET, E-Mail, UUCP and home of the
  Open Book Initiative (text project);  fees: 8a-6p $8/hr, 6p-12a $5/hr,
  12a-8a $2.50/hr;  Multiple lines: 2400 MNP used on listed number,
  Telebits used on others;  login as "new";  Contact: geb@world.std.com

07/88  619-444-7006^ pnet01     El Cajon        CA 3/12/24    24
  BSD Unix, 3 lines, login: pnet id: new, some USENET, email, conferencing
  Home of P-Net software, mail to crash!bblue or pnet01!bblue for info.
  Contributions requested
  Unix accounts available for regulars, PC Pursuit access 2/88.

10/88  703-281-7997^ grebyn     Vienna          VA 3/12/24/96  24
  Vax/Ultrix.  $25/month.  GNU EMACS, USENET, PC/BLUE archives, Telebit on 7998
  and 7999, archives, Ada repository, comp.sources.(misc,unix,games) archives,
  net.sources archives, 3 C compilers, Ada compiler,  500MB disk, multiple
  lines

11/89  708-272-5912^ igloo      Northbrook      IL 12/24/96    24
  3B2-300;  accounts by invitation only, no limit/no fee;  full usenet;
  132megs HD;  2 lines rotary, 9600 telebit on 272-5917
  Contact: igloo!postmaster

11/89  708-301-2100^ jolnet     Joliet          IL 3/12/24    24
  3b2/400 - Unix, public access and contributions, No fee for postnews.
  5 lines  AKCS bbs.  Free Newsfeeds available.  >450 MB online storage.
  Free Shell and Usenet access.  Telebit Trailblazer access (2104).
  Telenet access.

11/89  708-566-8911^ ddsw1      Mundelein       IL 3/12/24/96  24
  Televideo 386 -SCO XENIX 386, guest usr 1 hr daily, fee extends use
  AKCS bbs, fee $30/6 months $50/year, Authors of AKCS bbs
  multiple lines, 9600 bps available, anonymous uucp, >/README for info
  Contact: Karl Denninger (...!ddsw1!karl) Voice: (312) 566-8910

11/89  708-833-8126^ vpnet      Villa Park      IL 12/24/96    24
  386 Clone - Interactive 386/ix R2.0 (3.2), no fee. Akcs linked bbs
```

  including several Usenet conf's. No charge for shells. Trailblazer.
  Mail lisbon@vpnet.UUCP

07/89 713-438-5018   sugar   Houston   TX 3/12/24/96 24
  386/AT (2) networked – Bell Technologies V/386, usenet, news, downloads
  Homegrown BBS software, Trailblazer+ access, currently no charges

10/89 713-668-7176^ nuchat   Houston   TX 3/12/24/96 24
  i386; USENET, Mail, Shell Access; 300M On-line; Trailbazer Used;
  No fee.

12/88 714-635-2863   dhw68k   Anaheim   CA 12/24   24
  Unistride 2.1, no fee, also 714-385-1915, Trailblazer on both lines,
  USENET News, /bin/sh or /bin/csh available

05/89 714-662-7450   turnkey   Inglewood   CA 12/24   24
  286 – Xenix SYSV, XBBS

11/89 714-821-9671   alphacm   Cypress   CA 12/24/96   24
  386 – SCO-XENIX, no fee, Home of XBBS, 90 minute per login, 4 lines,
  9600 baud via MicroComm/Hayes (v.29)
    uucp-anon: ogin: nuucp NO PASSWD

05/89 714-842-5851   conexch   Santa Ana   CA 3/12/24   24
  386 – SCO Xenix – Free Unix guest login and PC-DOS bbs login, one
  hour inital time limit, USENET news, shell access granted on request &
  $25/quarter donation. Anon uucp: ogin: nuucp NO PASSWD. List of
  available Unix files resides in /usr3/public/FILES.

08/88 714-894-2246   stanton   Irvine   CA 3/12/24   24
  286 – SCO Xenix – donation requested, limit 240 min, XBBS, USENET news
  UNIX access granted on request through BBS, 20$/year, access includes
  C development system (XENIX/MSDOS), PROCALC 1-2-3 clone, FOXBASE+
  anon uucp: ogin: nuucp, no word, 2400/1200/300 MNP supported

05/88 719-632-4111   chariot   Colo Sprgs   CO 3/12   24
  Convrgnt Minifrme – SYS V, multiple lines, fee $12/mo Picospan

08/89 801-943-7947^ i-core   Salt Lake City   UT 3/12/24/96 24
  286 SYS V, Unidel BBS, a.k.a. Bitsko's Bar & Grill, no limit, no fee,
  UseNet and Citadel feeds available, home of Unidel BBS, Telebit 19200 used
  Contact: ken@i-core.UUCP or uunet!iconsys!caeco!i-core!ken

12/88 802-865-3614   tnl   Burlington   VT 3/12/24   24
  80386 w/ SCO XENIX. No Fee. 2 hr session limit. XBBS/USENET, shell.
  Login as 'new' for a shell account, no validation. AKA: Northern Lights.

08/88 813-952-1981   usource   Sarasota   FL 12/24   -24
  386 – SCO-XENIX, fee depends on services provided, no fee for bbs. New users
  subscribe by logging in as 'help' or 'newuser' (no password). Primary
  purpose is technical forum. 6pm-8am M-Th, 24 hrs weeekends (6pm Fri-8am Mon)
  uucp-anon: 1200/2400 bps --> ogin: auucp word: gateway
  uucp-anon directory: /usr/spool/uucppublic; contact: frank@usource.UUCP

08/88 814-333-6728   sir-alan   Meadville   PA 3/12/24   24
  Tandy XENIX/68000 03.01.02, Allegheny College, UNaXcess BBS
  uucp-anon: ogin: pdsrc NO PASSWD
  uucp-anon directory: /usr/spool/pdsrc/all.subjects
  Telebit TB+ available at 814 337 0894, now operating.
  Contact: sir-alan!mikes

05/88 814-337-3159   oncoast   Meadville   PA 3/12/24/96 24
  Tandy 12/6000, no fee, no bbs, archive site, USR HST 9600, cycle 24/96/12
  vols 1 – 13 of mod.sources/comp.sources.unix, comp.sources.misc
  New stuff on sir-alan, older on oncoast. 2 uucp logins "uucp" and "pdsrc"
  files list = /usr/spool/uucppublic/my.directory or /usr/spool/pdsrc/
  all.subjects.Z

09/89 916-649-0161   sactoh0   Sacramento   CA 12/24/96   24
  3B2/310 SYSV.2, SAC_UNIX; $2/month, limit 90 min, 2 lines, TB on line,

```
  2400/1200 baud on 916-722-6519;  USENET, E-Mail, Games;  login: new
  Contact: ..pacbell!sactoh0!sysop


089  919-493-7111^  wolves      Durham           NC  3/12/24       24
  AMS 386/25 - UNIX SysVr3.2, XBBS, no fee for bbs.  Rates for UNIX access
  and USENET are being determined.  Developing yet another UNIX bbs (ideas
  welcome!)  Single line, telebit coming soon.
  Contact: wolves!ggw or wolves!sysop  [...duke!dukcds!wolves!...]


--------------------------------------------------------------------------
NOTE:  ^ means the site is reachable using PC Pursuit.
==========================================================================
This list is maintained by Phil Eschallier on lgnp1.  Any additions, deletions,
or corrections should be sent to one of the addresses below.  The nixpub
listings are kept as current as possible.  However, you use this data at your
own risk and cost -- all standard disclaimers apply!!!
------
              Lists available from lgnp1 via anonomous uucp.
                     +1 215 348 9727 [Telebit access]
                  login: nuucp  NO PWD   [no rmail permitted]
                this list: /usr/spool/uucppublic/nixpub
                short list: /usr/spool/uucppublic/nixpub.short
          or from news groups pubnet.nixpub, comp.misc or alt.bbs.
------
E-MAIL ...
   uucp: ..!uunet!lgnp1!$ phil | nixpub $
     or: $ phil | nixpub $@LS.COM
    CIS: 71076,1576
==========================================================================
    COMPAQ, IBM, PC Pursuit, [SCO] XENIX, UNIX, etc. are trademarks of the
    respective companies.
==========================================================================


                        nixpub short listing
      Open Access UNIX (*NIX) Sites [Fee / No Fee] for mapped sites only
                        [ November 12, 1989 ]


Systems listed (73)
Legend:  fee/contribution ($), no fee (-$), hours (24), not (-24)
         shell (S), USENET news (N), email (M), multiple lines (T)
         Telebit 9600 bps on main number (+P), Telebit on other line[s] (P)
         Courier 9600 bps on main number (+H), Courier on other line[s] (H)
         anonymous uucp (A), archive site ONLY - see long form list (@)
         @> = anonymous uucp archive site listed in ANONIX (mike@cpmain)
         Dialable thru PC Pursuit (^)

Last
Contact
```

Date	Telephone #	Sys-name	Location		Baud	Legend
-----	------------	--------	----------		-------	---------
08/89	201-846-2460^	althea	New Brunswic	NJ	3/12/24	24 -$ M N S
10/89	206-328-4944	polari	Seatle	WA	3/12	24 $ M N P S T
10/89	212-420-0527	magpie	NYC	NY	3/12/24/96	24 -$ T P
10/89	212-675-7059	marob	NYC	NY	12/24	24 -$ A
05/89	212-879-9031^	dasys1	NYC	NY	12/24	24 $ S N M T
09/89	213-376-5714^	pnet02	Redondo Bch	CA	3/12/24	24 -$ M N T
09/89	213-397-3137^	stb	Santa Monica	CA	3/12/24	24 -$ S A
11/88	213-459-5891	amazing	Pac Palisade	CA	3/12/24	24 $ T
07/88	214-247-2367	ozdaltx	Dallas	TX	3/12/24	24 $ N T
07/89	214-741-2130	attctc	Dallas	TX	3/12/24	24 -$ N M S T A
11/89	215-348-9727	lgnp1	Doylestown	PA	3/12/24/96	24 $ A M N +P S
09/89	216-582-2441	ncoast	Cleveland	OH	12/24/96	24 $ S N M P T
08/88	217-529-3223	pallas	Springfield	IL	3/12/24	24 $ T
10/89	219-289-0286	nstar	South Bend	IN	3/12/24/96	24 -$ H M N P S T
08/88	312-283-0559^	chinet	Chicago	IL	3/12/24	24 $ N T
10/89	312-338-0632^	point	Chicago	IL	3/12/24/96	24 -$ N P S T
04/89	313-623-6309	nucleus	Clarkston	MI	12/24	24 $ S N M
11/88	313-994-6333	m-net	Ann Arbor	MI	3/12	24 $ T
08/89	313-996-4644^	anet	Ann Arbor	MI	3/12	24 $ T

```
08/89  314-474-4581   gensis    Columbia     MO  3/12/24/96   24 -$ M S
10/89  404-321-5020^  jdyx      Atlanta      GA  12/24        24 $ M N +P S T
05/88  407-380-6228   rtmvax    Orlando      FL  3/12/24      24 -$ N M
09/89  408-245-7726^  uuwest    Sunnyvale    CA  3/12/24      24 -$ N
04/88  408-247-4810   sharks    Santa Clara  CA  3/12         24 $ S N M T
11/89  408-423-9995   cruzio    Santa Cruz   CA  12/24        24 $ M T
10/89  408-725-0561^  portal    Cupertino    CA  3/12/24      24 $ -S N M T
02/89  408-997-9119^  netcom    San Jose     CA  3/12/24/96   24 $ M N S
10/89  412-431-8649   eklektik  Pittsburgh   PA  3/12/24      24 $ S N M
11/89  415-332-6106^  well      Sausalito    CA  12/24        24 $ M N S T
06/88  415-582-7691   cpro      Hayward      CA  12/24        24 -$ S
07/89  415-753-5265^  wet       San Francisc CA  3/12/24      24 $ M N S T
05/89  415-783-2543   esfenn    Hayward      CA  3/12/24      24 -$ M N S
01/89  416-452-0926   telly     Brampton     ON  12/24/96     +P 24 $ M N
12/88  416-461-2608   tmsoft    Toronto      ON  3/12/24/96   24 $ S M N
07/89  416-654-8854   ziebmef   Toronto      ON  3/12/24/96   24 +P M N S T
08/89  502-968-5401   disk      Louisville   KY  3/12         24 $ M N S T
12/88  503-254-0458   bucket    Portland     OR  3/12/24      24 -$ N M T
05/89  503-640-4262^  agora     PDX          OR  3/12/24      24 $ M N S T
10/88  512-346-2339   bigtex    Austin       TX  96           +P 24 -S -$ A @>
07/89  512-832-8835   rpp386    Austin       TX  12/24        24 @ -$ -S A T
10/89  513-779-8209   cinnet    Cincinnati   OH  12/24/96     24 $ M N +P S
05/89  516-872-2137   lilink    Long Island  NY  12/24        24 $ M N S T
07/89  517-487-3356   lunapark  E. Lansing   MI  12/24        24 -$
12/88  518-346-8033   sixhub    upstate      NY  3/12/24      24 $ S N M T
09/88  602-941-2005   xroads    Phoenix      AZ  3/12/24      24 $ N T
08/89  603-880-8120   ubbs-nh   Nashua       NH  3/12/24/96   24 -$ M N +P S T
08/89  605-348-2738   loft386   Rapid City   SD  3/12/24/96   24 $ M N +P S
08/88  608-273-2657   madnix    Madison      WI  3/12/24/96   24 -$ S N M
08/89  612-473-2295   pnet51    Minneapolis  MN  3/12/24      24 -$ N M T
08/89  615-896-8716   raider    Murfreesboro TN  12/24        24 -$ S N M T
07/89  616-457-1964   wybbs     Jenison      MI  3/12/24      24 -$ S N T
11/89  617-739-9753   world     Brookline    MA  3/12/24/96   24 $ M N P S T
07/88  619-444-7006^  pnet01    El Cajon     CA  3/12/24      24 $ N M S T
10/88  703-281-7997^  grebyn    Vienna       VA  3/12/24/96   24 $ N M T P
11/89  708-272-5912^  igloo     Northbrook   IL  12/24/96     24 -$ S N T P
11/89  708-301-2100^  jolnet    Joliet       IL  3/12/24      24 -$ +P M N S T
08/88  312-566-8911^  ddsw1     Mundelein    IL  3/12/24/96   24 $ S N M T A P
11/89  708-833-8126^  vpnet     Villa Park   IL  12/24/96     24 -$ +P M N S
07/89  713-438-5018   sugar     Houston      TX  3/12/24/96   24 -$ N +P
10/89  713-668-7176^  nuchat    Houston      TX  3/12/24/96   24 -$ M N +P S
12/88  714-635-2863   dhw68k    Anaheim      CA  12/24        24 -$ T
05/89  714-662-7450   turnkey   Inglewood    CA  12/24        24 -$
11/89  714-821-9671   alphacm   Cypress      CA  12/24/96     24 -$ T H A
05/89  714-842-5851   conexch   Santa Ana    CA  3/12/24      24 $ A M N S
08/88  714-894-2246   stanton   Irvine       CA  3/12/24      24 $ S N
05/88  719-632-4111   chariot   Colo Sprgs   CO  3/12         24 $ T
08/89  801-943-7947^  i-core    Salt Lake Ci UT  3/12/24/96   +P 24 -$ A N
06/88  802-865-3614   tnl       Burlington   VT  3/12/24      24 -$ S N M
08/88  813-952-1981   usource   Sarasota     FL  12/24        -24 -$ A
08/88  814-333-6728   sir-alan  Meadville    PA  3/12/24      24 -$ A P
05/88  814-337-3159   oncoast   Meadville    PA  3/12/24/96   +H 24 @ -$ -S A
09/89  916-649-0161   sactoh0   Sacramento   CA  12/24/96     24 $ M N +P S T
08/89  919-493-7111^  wolves    Durham       NC  3/12/24      24 $ M N S
-----------------------------------------------------------------------------
NOTE:  ^ means the site is reachable using PC Pursuit.
=============================================================================
```

This list is maintained by Phil Eschallier on lgnp1. Any additions, deletions,
or corrections should be sent to one of the addresses below. The nixpub
listings are kept as current as possible. However, you use this data at your
own risk and cost -- all standard disclaimers apply!!!

```
------
            Lists available from lgnp1 via anonomous uucp.
                +1 215 348 9727 [Telebit access]
              login:  nuucp  NO PWD   [no rmail permitted]
            this list:  /usr/spool/uucppublic/nixpub.short
            long list:  /usr/spool/uucppublic/nixpub
        or from news groups pubnet.nixpub, comp.misc or alt.bbs
------
E-MAIL ...
```

```
  uucp:  ..!uunet!lgnp1!{ phil │ nixpub }
    or:  { phil │ nixpub }@LS.COM
==============================================================================
  COMPAQ, IBM, PC Pursuit, [SCO] XENIX, UNIX, etc. are trademarks of the
  respective companies.


                  >---------=====END=====--------<
```

                        ==Phrack Inc.==

              Volume Three, Issue 29, File #5 of 12

        [-][-] [-][-] [-][-] [-][-] [-][-] [-][-] [-][-]
        [-]   [-]
        [-]   Covert Paths   [-]
        [-]   [-]
        [-]   by   [-]
        [-]   [-]
        [-]   Cyber Neuron Limited and Synthecide   [-]
        [-]   [-]
        [-]   November 1, 1989   [-]
        [-]   [-]
        [-][-] [-][-] [-][-] [-][-] [-][-] [-][-] [-][-]

When cracking a system, it is important for you to use a path to the system
that will not lead the authorities to your door step.

There are several methods for doing this and all of them will depend on your
destination, available time, goal and the phase of the moon. This article
deals mostly with cover attacks via a connected network.

If attacking via a phone link:

  o Tap in to your local payphone line and red box or "sprint" the call.

  o Using a long haul service (like Sprint or MCI) to dial into systems in
        remote cities. [This should hinder a track by a good order of
        magnitude.]

  o Use a midnight packet switching network (eg: PC-Pursuit, Tymnet, et. al.)

  o All the above.

If attacking from a network (eg: the Internet) there are ways of spoofing the
packet headers, but this requires superuser privileges on the system you are
attacking from and a fair amount of 'C' programming expertise. Therefore, this
will not be discussed here in any more detail.

Another obvious trick is to use network routers and gateways along with guest
accounts to "route" your data path. This will cause the person tracking you to
have to go though more red tape and hassle to track you. This gives you more
time to cover your tracks.

Some useful paths I know of are:

accuvax.nwu.edu
cory.berkeley.edu
violet.berkeley.edu
headcrash.berkeley.edu

    host: violet.berkeley.edu   host: headcrash.berkeley.edu
    account: nobody   account: netgate
    net address:128.32.136.22   net address: 128.32.234.31

    host: cory.berkeley.edu   host accuvax.nwu.edu
    account: terminal   account: telnet
    net address: 128.32.134.6   net address: 129.105.49.1

    host: lightning.berkeley.edu   host: score.stanford.edu
    port: 8033   account: guest
    net address: 128.32.234.10   net address: 36.8.0.46

The accounts nobody, netgate, and terminal at Berkeley are accounts that were
installed so that people can use the system to rlogin or telnet to an account
elsewhere without a local login (or so I am told by the local hackers [Hi
Audrey...]). The lightning path/method can be accessed by the command:
"telnet lightning.berkeley.edu 8033".

I am interested in hearing about other Internet access accounts that are
available out there. If you know of any please send them in.

Tymnet is also a useful method of gaining access to systems. From Tymnet, you
can hook up to just about any computer and use the other methods to go one step
further. It's not until you are traced back to the computer you linked to from
Tymnet that they can even begin to follow you back. My understanding is that
for a systen to find your Tymnet node, they must contact Tymnet personally and
ask them to put a trap on their connection.

For more infomation concerning Tymnet see the article "Hacking & Tymnet" by
Synthecide in Phrack Inc. Newsletter Issue XXX.

                 ****

                     >------=====END=====--------<

```
                    + BANK INFORMATION +
                  \                    /
                   \                  /
                    ___Compiled By___
                   /                  \
                    Legion Of Doom!
                     EFT Division
                     ------------
```

In order to exact any type of bank associated transaction by computer, one must
have a working knowledge of the various routing codes involved in the banking
processes. The following is an informational guide to the coding used in
American banking transactions.

ABA (American Bankers Association) Transit Numbers

Numbers 1 to 49 inclusive are Prefixes for Cities
Numbers 50 to 99 inclusive are Prefixes for States

Prefix Numbers 50 to 58 are Eastern States
Prefix Number 59 is for Alaska, Hawaii, and US Territories
Prefix Numbers 60 to 69 are Southeastern States
Prefix Numbers 70 to 79 are Central States
Prefix Numbers 80 to 88 are Southwestern States
Prefix Numbers 90 to 99 are Western States

1   New York, NY
2   Chicago, IL
3   Philadelphia, PA
4   St. Louis, MO
5   Boston, MA
6   Cleveland, OH
7   Baltimore, MD
8   Pittsburgh, PA
9   Detroit, MI
10   Buffalo, NY
11   San Francisco, CA
12   Milwaukee, WI
13   Cincinnati, OH
14   New Orleans, LA
15   Washington D.C.
16   Los Angeles, CA
18   Kansas City, MO
19   Seattle, WA
20   Indianapolis, IN
21   Louisville, KY
22   St. Paul, MN
23   Denver, CO
24   Portland, OR
25   Columbus, OH
26   Memphis, TN
27   Omaha, NE
28   Spokane, WA
29   Albany, NY
30   San Antonio, TX
31   Salt Lake City, UT
32   Dallas, TX
33   Des Moines, IA
34   Tacoma, WA
35   Houston, TX
36   St. Joseph, MO
37   Fort Worth, TX
38   Savannah, GA
39   Oklahoma City, OK
40   Wichita, KS
41   Sioux City, IA
```

```
42   Pueblo, CO
43   Lincoln, NE
44   Topeka, KS
45   Dubuque, IA
46   Galveston, TX
47   Cedar Rapids, IA
48   Waco, TX
49   Muskogee, OK
50   New York
51   Connecticut
52   Maine
53   Massachusetts
54   New Hampshire
55   New Jersey
56   Ohio
57   Rhode Island
58   Vermont
59   Alaska, American Samoa, Guam, Hawaii, Puerto Rico, Virgin Islands
60   Pennsylvania
61   Alabama
62   Delaware
63   Florida
64   Georgia
65   Maryland
66   North Carolina
67   South Carolina
68   Virginia
69   West Virginia
70   Illinois
71   Indiana
72   Iowa
73   Kentucky
74   Michigan
75   Minnesota
76   Nebraska
77   North Dakota
78   South Dakota
79   Wisconsin
80   Missouri
81   Arkansas
83   Kansas
84   Louisiana
85   Mississippi
86   Oklahoma
87   Tennessee
88   Texas
90   California
91   Arizona
92   Idaho
93   Montana
94   Nevada
95   New Mexico
96   Oregon
97   Utah
98   Washington
99   Wyoming
```

Federal Reserve Routing Symbols

```
     * All banks in an area served by a FR bank or branch bank
       carry the routing symbol of the FR bank or branch

1    Federal Reserve Bank of Boston Head        5-1
     Office                                     110

2    Federal Reserve Bank of New York Head      1-120
     Office                                      210

     Buffalo Branch                             10-26
```

		220
3	Federal Reserve Bank of Philadelphia Head Office	3-4 310
4	Federal Reserve Bank of Cleveland Head Office	0-1 410
	Cincinnati Branch	13-43 420
	Pittsburgh Branch	8-30 430
5	Federal Reserve Bank of Richmond Head Office	68-3 510
	Baltimore Branch	7-27 520
	Charlotte Branch	66-20 530
6	Federal Reserve Bank of Atlanta Head Office	64-14 610
	Birmingham Branch	61-19 620
	Jacksonville Branch	63-19 630
	Nashville Branch	87-10 640
	New Orleans Branch	14-21 650
7	Federal Reserve Bank of Chicago Head Office	2-30 710
	Detroit Branch	9-29 720
8	Federal Reserve Bank of St. Louis Head Office	4-4 810
	Little Rock Branch	81-13 110
	Louisville Branch	21-59 830
	Memphis Branch	26-3 840
9	Federal Reserve Bank of Minneapolis Head Office	17-8 910
	Helena Branch	92-26 920
10	Federal Reserve Bank of Kansas City Head Office	18-4 1010
	Denver Branch	23-19 1020
	Oklahoma City Branch	39-24 1030

```
        Omaha Branch                              27-12
                                                  1040

11   Federal Reserve Bank of Dallas Head          32-3
     Office                                       1110

        El Paso Branch                            88-1
                                                  1120

        Houston Branch                            35-4
                                                  1130

        San Antonio Branch                        30-72
                                                  1140

12   Federal Reserve Bank of San Francisco        11-37
     Head Office                                  1210

        Los Angeles Branch                        16-16
                                                  1220

        Portland Branch                           24-1
                                                  1230

        Salt Lake City Branch                     31-31
                                                  1240

        Seattle Branch                            19-1
                                                  1250
```

BANK IDENTIFICATION CODES


```
XX-YYY    WHERE:        XX = City or State
  ZZZZ                  YYY = Bank of Origin

                         ZZZZ = Federal Reserve Routing Code
```

If three digits: The first digit identifies the Federal Reserve District

                  The second digit, if 1, stands for the Head Office of the
                  Federal Reserve District; 2-5 stand for the Branch Office of
                  the Federal Reserve District

                  The third digit signifies: 0-available for immediate credit;
                  others have deferred credit and the digits mean the
                  following: 1-5 designates the state in which the drawee bank
                  is located; 6-9 special collection arrangements.

If four digits: The first two digits stand for the Federal Reserve District
                 10-12.

The following digits are as above

EXAMPLE:

```
68-424        68-State of Virginia
 514         424-Arlington Trust Co., Arlington, VA
               5-Fifth Federal Reserve District
               1-Head Office in Richmond, Virginia
               4-Deferred credit and the state of Virginia
```

*NOTE -- For further your familiarity with the coding process, on checks, these
        numbers appear at the bottom of the check according to the MICR Check
        Coding System. The check number, the account number, and the ABA
        Transit Number will all be encoded in magnetic ink. The ABA Number
        will be enclosed in symbols like: |: ABANUMBER |: The grouping of

the ABA and Federal Reserve Codes will also usually appear at the
upper right-hand corner of the check.

Keep in mind that there are a great many checks involved in any
banking procedure, and almost any transaction evoked improperly will
draw attention. Furthermore, the documents generated in a legitimate
wire-transfer situation are quite extensive. Should a transaction be
noticed, and these documents are not available for scrutiny, again
attention will be drawn to the situation.

                        * BANK DOCUMENTS *
                        * WIRE TRANSFER *

              INTERNAL   CUSTOMER RECORD

    Teller Tape & Proof Sheets   Copy of Wire Transfer Ticket
    Wire Transfer Ticket   Cancelled Check (if used to
    Microfilm copy of check   purchase)
      used to purchase wire   Bank Statement (if funds came
      transfer   out of the account)
    Microfilm copies of account
      records (if fund came out
      of existing account)
    Cash In/Out Ticket
    Vault Book Entry
    Bank Security Film
    Copy of CTR

Bank transactions must be swift and precise. Amounts should be kept under the
$10,000 range in order not to immediately arouse suspicion. Attacks must
executed correctly the first time, as there will be no possibilities for a
second chance. Monies must be gathered rapidly and dispersed into various
outlets to avoid additional attention. Transfers to banking systems whose
countries keep strict right to privacy laws, such as Panama, Switzerland,
et.al. are not recommended as the transactions are much more involved and there
exists a greater potential for error in international wire-transfers.

The preferred method of transfer of funds would involve one or more false
identities, complete with state approved identification or passport and social
security cards. Bank Security Film is kept on file, so it would be preferred
that some semblance of disguise be implemented, ranging from hair bleaching,
sun-tanning, makeup, false accents, facial hair, etc. Various accounts in the
assumed name would be opened in several cities with the minimum initial
balance. Within approximately two weeks, funds of no more than $7500 would be
diverted to each account. The funds would then be withdrawn in cash with no
more than $5000 from each account, the balance being left in the account. Once
the funds have been made cash, they would then be distributed to foreign banks,
or invested in foreign markets to avoid detection by the Internal Revenue
Service.

Conviction for Illegal Transference of Funds is not recommended.

                >-------=====END=====--------<

==Phrack Inc.==

Volume Three, Issue 29, File #7 of 12

The Legion of Doom!
EFT Division

Presents

HOW WE GOT RICH THROUGH ELECTRONIC FUND TRANSFERS

(OR: GEE! NO, GTE!)

     A certain number of financial institutions that reside within the
packet-switched confines of the various X.25 networks use their connections to
transfer funds from one account to another, one mutual fund to another, one
stock to another, one bank to another, etc... It is conceivable that if one
could intercept these transactions and divert them into another account, they
would be transferred (and could be withdrawn) before the computer error was
noticed. Thus, with greed in our hearts, an associate and I set forth to test
this theory and conquer the international banking world.

     We chose CitiCorp as our victim. This multinational had two address
prefixes of its own on Telenet (223 & 224). Starting with those two prefixes,
my associate and I began to sequentially try every possible address. We
continued through 1000 in increments of one, then A-Z, then 1000-10000 by 10's,
and finally 10000-99999 by 100's. Needless to say, many addresses were
probably skipped over in our haste to find valid ones, but many we passed over
were most likely duplicate terminals that we had already encountered.

     For the next few days my associate and I went over the addresses we had
found, comparing and exchanging information, and going back to the addresses
that had shown 'NOT OPERATING,' 'REMOTE PROCEDURE ERROR,' and 'REJECTING.' We
had discovered many of the same types of systems, mostly VAX/VMS's and Primes.
We managed to get into eight of the VAXen and then went forth on the CitiCorp
DECNET, discovering many more. We entered several GS1 gateways and Decservers
and found that there were also links leading to systems belonging to other
financial institutions such as Dai-Ichi Kangyo Bank New York and Chase
Manhattan. We also found hundreds of addresses to TWX machines and many
in-house bank terminals (most of which were 'BUSY' during banking hours, and
'NOT OPERATING' during off hours). In fact, the only way we knew that these
were bank terminals was that an operator happened to be idle just as I
connected with her terminal (almost like the Whoopie Goldberg movie, "Jumpin'
Jack Flash," not quite as glamorous ...yet.)

     Many of the computers we eventually did penetrate kept alluding to the
electronic fund transfer in scripts, files, and personal mail. One of the
TOPS-20 machines we found even had an account EFTMKTG.EFT, (password EFTEFT)!
All the traces pointed to a terminal (or series of terminals) that did nothing
but transfer funds. We decided that this was the case and decided to
concentrate our efforts on addresses that allowed us to CONNECT periodically
but did not respond. After another week of concentrated effort, we managed to
sort through these. Many were just terminals that had been down or
malfunctioning, but there were five left that we still had no idea of their
function. My associate said that we might be able to monitor data
transmissions on the addresses if we could get into the debug port. With this
idea in mind, we set out trying sub-addresses from .00 to .99 on the mystery
addresses. Four of the five had their debug ports at the default location
(.99). The fifth was located 23 away from the default. That intrigued us, so
we put the others aside and concentrated on the fifth. Although its location
was moved, a default password was still intact, and we entered surreptitiously.

     The system was menu driven with several options available. One option,
Administrative Functions, put us into a UNIX shell with root privilege. After
an hour or so of nosing around, we found a directory that held the Telenet
Debug Tools package (which I had previously thought existed solely for Prime
computers). Using TDT, we were able to divert all data (incoming and outgoing)
into a file so we could later read and analyze it. We named the file ".trans"
and placed it in a directory named ".. ", (dot, dot, space, space) so it would

remain hidden. This was accomplished fairly late on a Sunday night. After
logging off, we opened a case of Coors Light and spent the rest of the night
(and part of the morning!) theorizing about what we might see tomorrow night
(and getting rather drunk).

     At approximately 9:00 p.m. the following evening, we met again and logged
onto the system to view the capture file, hoping to find something useful. We
didn't have to look very far! The first transmission was just what we had been
dreaming about all along. The computer we were monitoring initiated by
connecting with a similar computer at another institution, waited for a
particular control sequence to be sent, and then transferred a long sequence of
numbers and letters. We captured about 170 different transactions on the first
day and several hundred more in the following week. After one business week,
we removed the file and directory, killed the TDT routine, and went through the
system removing all traces that we had been there.

     We felt that we had enough to start piecing together what it all meant, so
we uploaded our findings to the LOD HP-3000 (ARMA) in Turkey. This way we
could both have access to the data, but keep it off our home systems. We
didn't bother to tell any of the other LOD members about our doings, as most
had retired, been busted, or were suspected of turning information over to the
Secret Service. Using this as a base, we analyzed the findings, sorted them,
looked for strings being sent, etc.

     We came to the conclusion that the transmissions were being sent in the
following way:

     XXXXXXXXXXXXTCxxxxxxxxxxxx/NNNNNNNNNNNNCnnnnnnnnnnnnnAMzzzzzzz.zzOP#
     X=Originating Bank ID
     T=Transfer (Also could be R(ecieve), I(nquire))
     C=Type of account (Checking--Also S(avings) I(RA) M(oney Market)
         T(rust) W(Other wire transfer ie. Credit Transfer, etc.))
     x=Originating Account Number
     /=Slash to divide string
     N=Destination Bank ID
     C=Type of account (See above)
     n=Destination Account Number
     AMzzzzzzz.zz=Amount followed by dollar and cents amount
     OP#=operator number supervising transaction

     After this string of information was sent, the destination bank would then
echo back the transaction and, in ten seconds, unless a CONTROL-X was sent,
would send "TRANSACTION COMPLETED" followed by the Destination Bank ID.

     We now needed to check out our theory about the Bank ID's, which I figured
were the Federal Reserve number for the Bank. Every bank in America that deals
with the Federal Reserve System has such a number assigned to it (as do several
European Banks). I called up CitiBank and inquired about their Federal Reserve
Number. It was the number being sent by the computer. With this information,
we were ready to start.

     I consulted an accountant friend of mine for information on Swiss or
Bahamanian bank accounts. He laughed and said that a $50,000 initial deposit
was required to get a numbered account at most major Swiss banks. I told him
to obtain the forms necessary to start the ball rolling and I'd wire the money
over to the bank as soon as I was told my account number. This shook him up
considerably, but he knew me well enough not to ask for details. He did,
however, remind me of his $1000 consulting fee. A few days later he showed up
at my townhouse with an account number, several transaction slips and
paperwork. Knowing that I was up to something shady, he had used one of his
own false identities to set up the account. He also raised his "fee" to $6500
(which was, amazingly enough, the amount he owed on his wife's BMW).

     My associate and I then flew to Oklahoma City to visit the hall of records
to get new birth certificates. With these, we obtained new State ID's and
Social Security Numbers. The next step was to set up bank accounts of our own.
My associate took off to Houston and I went to Dallas. We each opened new
commercial accounts at three different banks as LOD Inc. with $1000 cash.

     Early the next day, armed with one Swiss and six American accounts, we
began our attack. We rigged the CitiCorp computer to direct all of its data
flow to a local Telenet node, high up in the hunt series. Amazingly, it still
allowed for connections from non-909/910 nodes. We took turns sitting on the
node, collecting the transmissions and returning the correct acknowledgments.
By 12:30 we had $184,300 in electronic funds in "Limbo." Next we turned off
the data "forwarding" on the CitiCorp computer and took control of the host
computer itself through the debug port to distribute the funds. Using its data
lines, we sent all the transactions, altering the intended bank destinations,
to our Swiss account.

     After I got the confirmation from the Swiss bank I immediately filled out
six withdrawal forms and faxed them to the New York branch of the Swiss bank
along with instructions on where the funds should be distributed. I told the
bank to send $7333 to each of our six accounts (this amount being small enough
not to set off Federal alarms). I did this for three consecutive days, leaving
our Swiss account with $52,000. I signed a final withdrawal slip and gave it
to my accountant friend.

     Over the next week we withdrew the $22,000 from each of our Dallas and
Houston banks in lots of $5000 per day, leaving $1000 in each account when we
were through. We were now $66,000 apiece richer.

     It will be interesting to see how the CitiCorp Internal Fraud Auditors and
the Treasury Department sort this out. There are no traces of the diversion,
it just seems to have happened. CitiBank has printed proof that the funds were
sent to the correct banks, and the correct banks acknowledgment on the same
printout. The correct destination banks, however, have no record of the
transaction. There is record of CitiBank sending funds to our Swiss account,
but only the Swiss have those records. Since we were controlling the host when
the transactions were sent, there were no printouts on the sending side. Since
we were not actually at a terminal connected to one of their line printers, no
one should figure out to start contacting Swiss banks, and since CitiBank does
this sort of thing daily with large European banks, they will be all twisted
and confused by the time they find ours. Should they even get to our bank,
they will then have to start the long and tedious process of extracting
information from the Swiss. Then if they get the Swiss to cooperate, they will
have a dead-end with the account, since it was set up under the guise of a
non-entity. The accounts in Dallas and Houston were also in fake names with
fake Social Security Numbers; we even changed our appearances and handwriting
styles at each bank.

     I'm glad I'm not the one who will have the job of tracking me down, or
even trying to muster up proof of what happened. Now we won't have to worry
about disposable income for awhile. I can finish college without working and
still live in relative luxury. It's kind of weird having over six-hundred $100
bills in a drawer, though. Too bad we can't earn any interest on it!

**   Since the events described transpired, CitiBank has made their Banking
     Transaction Ports all refuse collect connections. Even by connecting
     with an NUI they now respond "<<ENTER PASSWORD>>". C'est La Vie.

                    >-------=====END=====--------<

==Phrack Inc.==

Volume Three, Issue 29, File #8 of 12

```
.................................................
||||||!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!||||||
|||!!!                                !!!|||
|||      The Myth and Reality About      |||
|||           Eavesdropping               |||
|||                                       |||
|||         by Phone Phanatic             |||
|||                                       |||
|||...      October 8, 1989      ...|||
||||||...............................||||||
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Most Central Office (CO) eavesdropping intercepts in a Bell Operating Company
(BOC) CO are today performed using a modified Metallic Facility Termination
(MFT) circuit pack which places about a 100,000 ohm isolated bridging impedance
across the subscriber line. Supervisory signaling is detected on the
subscriber loop using a high-impedance electronic circuit, and the signaling is
repeated in an isolated fashion using the A and B leads of the repeating coil
in the MFT to "reconstruct" a CO line for the benefit of monitoring apparatus.

The entire purpose of the above effort is to prevent any trouble or noise on
the intercept line or monitoring apparatus from causing any trouble, noise or
transmission impairment on the subject line.

Some BOCs may elect to use service observing apparatus to provide the necessary
isolation and repeated loop supervisory signaling. Less common are locally
engineered variations which merely use an isolation amplifier from an MFT or
other 4-wire repeater, and which provide no repeated supervisory signaling
(which is not all that necessary, since voice-activated recorders and DTMF
signaling detectors can be used, and since dial pulses can be counted by
playing a tape at slow speed).

Today, the use of a "bridge lifter" retardation coil for the purpose of
connecting an eavesdropping intercept line is virtually non-existent since they
do not provide sufficient isolation and since they provide a fair amount of
insertion loss without loop current on the "observing" side. Bridge lifter
coils are primarily intended for answering service intercept lines, and consist
of a dual-winding inductor which passes 20 Hz ringing and whose windings easily
saturate when DC current flows. Bridge lifter coils are used to minimize the
loading effect (and consequent transmission impairment) of two subscriber loops
on one CO line. Bridge lifter coils provide a significant insertion loss at
voice frequencies toward the idle loop; i.e., the loop in use will have DC
current flow, saturating the inductor, and reducing its insertion loss to
1.0 dB or less.

Despite gadget advertised in magazines like The Sharper Image, the simple truth
of the matter is that there is NO WAY for any person using ANY type of
apparatus at the telephone set location to ascertain whether there is a
properly installed eavesdropping device connected across their line in the CO.
The only way such a determination can be made is through the cooperation of the
telephone company.

For that matter, there is virtually no way for any person using any type of
apparatus in their premises to ascertain if there is ANY type of eavesdropping
apparatus installed ANYWHERE on their telephone line outside their premises,
unless the eavesdropping apparatus was designed or installed in an
exceptionally crude manner (not likely today). Some types of eavesdropping
apparatus may be located, but only with the full cooperation of the telephone
company.

The sole capability of these nonsense gadgets is to ascertain if an extension
telephone is picked up during a telephone call, which is hardly a likely
scenario for serious eavesdropping!

These screw-in-the-handset gadgets work by sensing the voltage across the

carbon transmitter circuit, and using a control to null this voltage using a comparator circuit. When a person makes a telephone call, the control is adjusted until the light just goes out. If an extension telephone at the user's end is picked up during the call, the increased current drain of a second telephone set will decrease the voltage across the carbon transmitter circuit, unbalancing the voltage comparator circuit, and thereby causing the LED to light.

These voltage comparator "tap detectors" cannot even be left with their setpoint control in the same position, because the effective voltage across a subscriber loop will vary depending upon the nature of the call (except in the case of an all digital CO), and upon other conditions in the CO. Electromechanical and analog ESS CO's may present different characteristics to the telephone line, depending upon whether it is used at the time of: An originated intraoffice call (calling side of intraoffice trunk), an answered intraoffice call (called side of intraoffice trunk), an originated tandem call (interoffice tandem trunk), an originated toll call (toll trunk), or an answered tandem/toll call (incoming tandem or toll trunk). There is usually enough variation in battery feed resistance due to design and component tolerance changes on these different trunks to cause a variation of up to several volts measured at the subscriber end for a given loop and given telephone instrument.

Even more significant are variations in CO battery voltage, which can vary (within "normal limits") from 48 volts to slightly over 52 volts, depending upon CO load conditions. 50 to 51 volts in most CO's is a typical daily variation. If anyone is curious, connect an isolated voltage recorder or data logger to a CO loop and watch the on-hook voltage variations; in many CO's the resultant voltage vs 24-hour time curve will look just like the inverse of a busy-hour graph from a telephone traffic engineering text!

In some all-digital CO apparatus, the subscriber loop signaling is performed by a solid-state circuit which functions as a constant-current (or current-limiting) device. With such a solid-state circuit controlling loop current, there is no longer ANY meaningful reference to CO battery voltage; i.e., one cannot even use short-circuit loop current at the subscriber location to even estimate outside cable plant resistance.

To explode this myth even further, let's do a little Ohm's Law:

1. Assume a CO loop with battery fed from a dual-winding A-relay (or line relay, ESS ferrod line scanner element, or whatever) having 200 ohms to CO battery and 200 ohms to ground.

2. Assume a CO loop of 500 ohms (a pretty typical loop).

3. Assume an eavesdropping device with a DC resistance of 100,000 ohms (this is still pretty crude, but I'm being generous with my example).

4. Using some simple Ohm's law, the presence or absence of this hypothetical eavesdropping device at the SUBSCRIBER PREMISES will result in a voltage change of less than 0.5 volt when measured in the on-hook state. This voltage change is much less than normal variations of CO battery voltage.

5. Using some simple Ohm's law, the presence or absence of this hypothetical eavesdropping device at the CENTRAL OFFICE LOCATION will result in a voltage change of less than 0.2 volt when measured in the on-hook state. This voltage change is an order of magnitude less than the expected normal variation of CO battery voltage!

Measuring voltage variations on a subscriber loop in an effort to detect a state-of-the-art eavesdropping device is meaningless, regardless of resolution of a voltage measuring device, since the "signal" is in effect buried in the "noise".

Moving on to the subject of subscriber line impedance...

There is simply no way for any device located on the subscriber's premises to obtain any MEANINGFUL information concerning the impedance characteristics of

the subscriber loop and whether or not anything "unusual" is connected at the CO (or for that matter, anywhere else on the subscriber loop). There are a number of reasons why this is the case, which include but are not limited to:

1. The impedance of a typical telephone cable pair results from distributed impedance elements, and not lumped elements. Non-loaded exchange area cable (22 to 26 AWG @ 0.083 uF/mile capacitance) is generally considered to have a characteristic impedance of 600 ohms (it actually varies, but this is a good compromise figure). Loaded exchange area cable, such as H88 loading which are 88 mH coils spaced at 6 kft intervals, is generally considered to have a a characteristic impedance of 900 ohms (it actually varies between 800 and 1,200 ohms, but 900 ohms is generally regarded as a good compromise figure for the voice frequency range of 300 to 3,000 Hz). What this means is that a bridged impedance of 100,000 ohms located in the CO on a typical subscriber loop will result in an impedance change measured at the SUBSCRIBER LOCATION of 0.1% or less. That's IF you could measure the impedance change at the subscriber location.

2. As a general rule of thumb, the impedance of an exchange area telephone cable pair changes ONE PERCENT for every TEN DEGREES Fahrenheit temperature change. Actual impedance changes are a function of the frequency at which the impedance is measured, but the above rule is pretty close for the purposes of this discussion.

3. Moisture in the telephone cable causes dramatic changes in its impedance characteristics. While this may appear obvious in the case of pulp (i.e., paper) insulated conductors, it is also characteristic of polyethylene (PIC) insulated conductors. Only gel-filled cable (icky-PIC), which still represents only a small percentage of installed cable plant, is relatively immune from the effects of moisture.

4. From a practical standpoint, it is extremely difficult to measure impedance in the presence of the DC potential which is ALWAYS found on a telephone line. The subscriber has no means to remove the telephone pair from the switching apparatus in the CO to eliminate this potential.

    Therefore, any attempt at impedance measurement will be subject to DC current saturation error of any inductive elements found in an impedance bridge. The telephone company can, of course, isolate the subscriber cable pair from the switching apparatus for the purpose of taking a measurement -- but the subscriber cannot. In addition to the DC current problem, there is also the problem of impulse and other types of noise pickup on a connected loop which will impress errors in the impedance bridge detector circuit. Such noise primarily results from the on-hook battery feed, and is present even in ESS offices, with ferrod scanner pulses being a good source of such noise. While one could possibly dial a telephone company "balance termination" test line to get a quieter battery feed, this still leaves something to be desired for any actual impedance measurements.

5. Devices which connect to a telephone pair and use a 2-wire/4-wire hybrid with either a white noise source or a swept oscillator on one side and a frequency-selective voltmeter on the other side to make a frequency vs return loss plot provide impressive, but meaningless data. Such a plot may be alleged to show "changes" in telephone line impedance characteristics. There is actual test equipment used by telephone companies which functions in this manner to measure 2-wire Echo Return Loss (ERL), but the ERL measurement is meaningless for localization of eavesdropping devices.

6. It is not uncommon for the routing of a subscriber line cable pair to change one or more times during its lifetime due to construction and modification of outside cable plant. Outside cable plant bridge taps (not of the eavesdropping variety) can come and go, along with back taps in the CO to provide uninterrupted service during new cable plant additions. Not only can the "active" length of an existing cable pair change by several percent due to construction, but lumped elements of

impedance can come and go due to temporary or permanent bridge taps.

The bottom line of the above is that one cannot accurately measure the
impedance of a telephone pair while it is connected to the CO switching
apparatus, and even if one could, the impedance changes caused by the
installation of an eavesdropping device will be dwarfed by changes in cable
pair impedance caused by temperature, moisture, and cable plant construction
unknown to the subscriber.

About a year ago on a bulletin board I remember some discussions in which there
was mention of the use of a time domain reflectometer (TDR) for localization of
bridge taps and other anomalies. While a TDR will provide a rather detailed
"signature" of a cable pair, it has serious limitations which include, but are
not limited to:

    1. A TDR, in general, cannot be operated on a cable pair upon which there
        is a foreign potential; i.e., a TDR cannot be used on a subscriber
        cable pair which is connected to the CO switching apparatus.

    2. A TDR contains some rather sensitive circuitry used to detect the
        reflected pulse energy, and such circuitry is extremely susceptible to
        noise found in twisted pair telephone cable. A TDR is works well with
        coaxial cable and waveguide, which are in effect shielded transmission
        lines. The use of a TDR with a twisted cable pair is a reasonable
        compromise provided it is a _single_ cable pair within one shield.
        The use of a TDR with a twisted cable pair sharing a common shield
        with working cable pairs is an invitation to interference by virtue of
        inductive and capacitive coupling of noise from the working pairs.

    3. Noise susceptibility issues notwithstanding, most TDR's cannot be used
        beyond the first loading coil on a subscriber loop since the loading
        coil inductance presents far too much reactance to the short pulses
        transmitted by the TDR. There are one or two TDR's on the market
        which claim to function to beyond ONE loading coil, but their
        sensitivity is poor.

There is simply no device available to a telephone subscriber that without the
cooperation of the telephone company which can confirm or deny the presence of
any eavesdropping device at any point beyond the immediate premises of the
subscriber. I say "immediate premises of the subscriber" because one presumes
that the subscriber has the ability to isolate the premises wiring from the
outside cable plant, and therefore has complete inspection control over the
premises wiring.

I have used the phrase "without the cooperation of the telephone company"
several times in this article. No voltage, impedance or TDR data is meaningful
without knowing the actual circuit layout of the subscriber loop in question.
Circuit layout information includes such data as exact length and guages of
loop sections, detailed description of loading (if present), presence and
location of multiples and bridge taps, calculated and measured resistance of
the loop, loop transmission loss, etc. There is NO way that a telephone
company is going to furnish that information to a subscriber! Sometimes it's
even difficult for a government agency to get this information without judicial
intervention.

Despite what I have stated in this article, you will see claims made by third
parties as to the existence of devices which will detect the presence of
telephone line eavesdropping beyond the subscriber's immediate premises. With
the exception of the trivial cases of serious DC current draw by an extension
telephone or the detection of RF energy emitted by a transmitter, this just
ain't so. Companies like Communication Control Corporation (which advertises
in various "executive" business publications) get rich by selling devices which
claim to measure minute voltage and impedance changes on a telephone line --
but consider those claims in view of the voltage changes due to CO battery
variations and due to temperature changes in outside cable plant -- and you
should get the true picture.

                    >-----------=====END============-----<

                      ==Phrack Inc.==

            Volume Three, Issue 29, File #9 of 12

    \'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\
     \'\   \'\
     \'\   BLOCKING OF LONG-DISTANCE CALLS... REVISITED   \'\
     \'\   by Jim Schmickley   \'\
     \'\   \'\
     \'\   Hawkeye PC, Cedar Rapids, Iowa   \'\
     \'\   \'\
     \'\   Previosly Seen in Pirate Magazine   \'\
     \'\   \'\
    \'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\`\'\

This file is a continuation of "Block Of Long-Distance Calls" that was seen in
Phrack Inc. Issue 21, file 8. Although the material has already been released
(perhaps on a limited basis) in Pirate Magazine, we felt the information was
important enough to re-present (on a larger scale), especially considering it
was an issue that we had previously detailed. -- Phrack Inc. Staff

The following article begins where the previous article left off:

- -

                                                   November 17, 1988

Customer Service
Teleconnect
P.O. Box 3013
Cedar Rapids, IA 52406-9101

Dear Persons:

I am writing in response to my October Teleconnect bill, due November 13, for
$120.76. As you can see, it has not yet been paid, and I would hope to delay
payment until we can come to some equitable table resolution of what appears to
be a dispute.   The records should show that I have paid previous bills
responsibly. Hence, this is neither an attempt to delay nor avoid payment. My
account number is: 01-xxxx-xxxxxx. My user phone is: 815-xxx-xxxx. The phone
of record (under which the account is registered) is: 815-xxx-xxxx.

If possible, you might "flag" my bill so I will not begin receiving dunning
notices until we resolve the problem. I have several complaints. One is the
bill itself, the other is the service. I feel my bill has been inflated
because of the poor quality of the service you provide to certain areas of the
country. These lines are computer lines, and those over which the dispute
occurs are 2400 baud lines. Dropping down to 1200 baud does not help much. As
you can see from my bill, there are numerous repeat calls made to the same
location within a short period of time. The primary problems occured to the
following locations:

1. Highland, CA   714-864-4592
2. Montgomery, AL   205-279-6549
3. Fairbanks, AK   907-479-7215
4. Lubbock, TX   806-794-4362
5. Perrine, FL   305-235-1645
6. Jacksonville, FL   904-721-1166
7. San Marcos, TX   512-754-8182
8. Birmingham, AL   205-979-8409
9. N. Phoenix, AZ   602-789-9269 <-- (The Dark Side BBS by The Dictator)

The problem is simply that, to these destinations, Teleconnect can simply not
hold a line. AT&T can. Although some of these destinations were held for a
few minutes, generally, I cannot depend on TC service, and have more recently
begun using AT&T instead. Even though it may appear from the records that I
maintained some contact for several minutes, this time was useless, because I

cold not complete my business, and the time was wasted. An equitable
resolution would be to strike these charges from my bill.

I would also hope that the calls I place through AT&T to these destinations
will be discounted, rather than pay the full cost. I have enclosed my latest
AT&T bill, which includes calls that I made through them because of either
blocking or lack of quality service. If I read it correctly, no discount was
taken off. Is this correct?

As you can see from the above list of numbers, there is a pattern in the poor
quality service: The problem seems to lie in Western states and in the deep
south. I have no problem with the midwest or with numbers in the east.

I have been told that I should call a service representative when I have
problems. This, however, is not an answer for several reasons. First, I have
no time to continue to call for service in the middle of a project. The calls
tend to be late at night, and time is precious. Second, on those times I have
called, I either could not get through, or was put on hold for an
indeterminable time.   Fourth, judging from comments I have received in several
calls to Teleconnect's service representatives, these seem to be problems for
which there is no immediate solution, thus making repeated calls simply a waste
of time. Finally, the number of calls on which I would be required to seek
assistance would be excessive. The inability to hold a line does not seem to
be an occasional anomaly, but a systematic pattern that suggests that the
service to these areas is, indeed, inadequate.

A second problem concerns the Teleconnect policy of blocking certain numbers.
Blocking is unacceptable. When calling a blocked number, all one receives is a
recorded message that "this is a local call." Although I have complained about
this once I learned of the intentional blocking, the message remained the same.
I was told that one number (301-843-5052) would be unblocked, and for several
hours it was. Then the blocking resumed.

A public utility simply does not have the right to determine who its customers
may or may not call. This constitutes a form of censorship. You should
candidly tell your customers that you must approve of their calls or you will
not place them. You also have the obligation to provide your customers with a
list of those numbers you will not service so that they will not waste their
time attempting to call. You might also change the message that indicates a
blocked call by saying something "we don't approve of who you're calling, and
won't let you call."

I appreciate the need to protect your customers. However, blocking numbers is
not appropriate. It is not clear how blocking aids your investigation, or how
blocking will eliminate whatever problems impelled the action. I request the
following:

1. Unblock the numbers currently blocked.
2. Provide me with a complete list of the numbers you are blocking.
3. End the policy of blocking.

I feel Teleconnect has been less than honest with its customers, and is a bit
precipitous in trampling on rights, even in a worthy attempt to protect them
from abuses of telephone cheats. However, the poor quality of line service,
combined with the apparrent violation of Constitutional rights, cannot be
tolerated. Those with whom I have spoken about this matter are polite, but the
bottom line is that they do not respond to the problem. I would prefer to pay
my bill only after we resolve this.

Cheerfully,

(Name removed by request)

- -

```
            /*/ ST*ZMAG SPECIAL REPORT - by Jerry Cross /*/
                  (reprinted from Vol. #28, 7 July, 1989)
            ===============================================
                  TELECONNECT CALL BLOCKING UPDATE
                      Ctsy (Genesee Atari Group)
```

Background
~~~~~~~~~~

At the beginning of last year one of my bbs users uploaded a file he found on
another bbs that he thought I would be interested in. It detailed the story of
an Iowa bbs operator who discovered that Teleconnect, a long distance carrier,
was blocking incoming calls to his bbs without his or the callers knowledge.

As an employee of Michigan Bell I was very interested. I could not understand
how a company could interfere with the transmissions of telephone calls,
something that was completely unheard of with either AT&T or Michigan Bell in
the past. The calls were being blocked, according to Teleconnect public
relations officials, because large amounts of fraudulent calls were being
placed through their system. Rather than attempting to discover who was
placing these calls, Teleconnect decided to take the easy (and cheap) way out
by simply block access to the number they were calling. But the main point was
that a long distance company was intercepting phone calls. I was very
concerned.

I did some investigating around the Michigan area to see what the long distance
carriers were doing, and if they, too, were intercepting or blocking phone
calls. I also discovered that Teleconnect was just in the process of setting
up shop to serve Michigan. Remember, too, that many of the former AT&T
customers who did not specify which long distance carrier they wanted at the
time of the AT&T breakup were placed into a pool, and divided up by the
competing long distance companies. There are a number of Michigan users who
are using certain long distance carriers not of their choice.

My investigation discovered that Michigan Bell and AT&T have a solid, computer
backed security system that makes it unnecessary for them to block calls. MCI,
Sprint, and a few other companies would not comment or kept passing me around
to other departments, or refused to comment about security measures.

I also discussed this with Michigan Bell Security and was informed that any
long distance company that needed help investigating call fraud would not only
receive help, but MBT would actually prepare the case and appear in court for
prosecution!

My calls to Teleconnect were simply ignored. Letters to the public service
commission, FCC, and other government departments were also ignored. I did,
however, get some cooperation from our U.S. Representative Dale Kildee, who
filed a complaint in my name to the FCC and the Interstate Commerce Commission.
What follows is their summary of an FCC investigation to Mr. Kildee's office.

- -

Dear Congressman Kildee:

This is in further response to your October 18, 1988 memorandum enclosing
correspondence from Mr. Gerald R. Cross, President of the Genesee Atari Group
in Flint, Michigan concerning a reported incidence of blocking calls from
access to Curt Kyhl's Stock Exchange Bulletin Board System in Waterloo, Iowa by
Teleconnect, a long distance carrier. Mr. Cross, who also operates a bulletin
board system (bbs), attaches information indicating that Teleconnect blocked
callers from access via its network to Mr. Kyhl's BBS number in an effort to
prevent unauthorized use of its customers' long distance calling authorization
codes by computer "hackers." Mr. Cross is concerned that this type of blocking
may be occurring in Michigan and that such practice could easily spread
nationwide, thereby preventing access to BBSs by legitimate computer users.

On November 7, 1988, the Informal Complaints Branch of the Common Carrier
Bureau directed Teleconnect to investigate Mr. Cross' concerns and report the
results of its investigation to this Commission. Enclosed, for your
information, is a copy of Teleconnect's December 7, 1988 report and its
response to a similar complaint filed with this Commission by Mr. James
Schmickley. In accordance with the commission's rules, the carrier should have
forwarded a copy of its December 7, 1988 report to Mr. Cross at the same time
this report was filed with the Commission. I apologize for the delay in
reporting the results of our investigation to your office.

Teleconnect's report states that it is subject to fraudulent use of its network
by individuals who use BBSs in order to unlawfully obtain personal
authorization codes of consumers. Teleconnect also states that computer
"hackers" employ a series of calling patterns to access a carrier's network in
order to steal long distance services. The report further states that
Teleconnect monitors calling patterns on a 24 hour basis in an effort to
control, and eliminate when possible, code abuse. As a result of this
monitoring, Teleconnect advises that its internal security staff detected
repeated attempts to access the BBS numbers in question using multiple
seven-digit access codes of legitimate Teleconnect customers. These calling
patterns, according to Teleconnect, clearly indicated that theft of
telecommunications services was occurring.

The report states that Teleconnect makes a decision to block calls when the
estimated loss of revenue reaches at least $500. Teleconnect notes that
blocking is only initiated when signs of "hacking" and other unauthorized usage
are present, when local calls are attempted over its long distance network or
when a customer or other carrier has requested blocking of a certain number.
Teleconnect maintains that blocking is in compliance with the provisions of
Section A.20.a.04 of Teleconnect's Tariff FCC No. #3 which provides that
service may be refused or disconnected without prior notice by Teleconnect for
fraudulent unauthorized use. The report also states that Teleconnect customers
whose authorizations codes have been fraudulently used are immediately notified
of such unauthorized use and are issued new access codes. Teleconnect further
states that while an investigation is pending, customers are given instructions
on how to utilize an alternative carrier's network by using "10XXX" carrier
codes to access interstate or intrastate communications until blocking can be
safely lifted.

Teleconnect maintains that although its tariff does not require prior notice to
the number targeted to be blocked, it does, in the case of a BBS, attempt to
identify and contact the Systems Operator (SysOp), since the SysOp will often
be able to assist in the apprehension of an unauthorized user. The report
states that with regard to Mr. Kyle's Iowa BBS, Teleconnect was unable to
identify Mr. Kyle as the owner of the targeted number because the number was
unlisted and Mr. Kyhl's local carrier was not authorized to and did not release
any information to Teleconnect by which identification could be made. The
report also states that Teleconnect attempted to directly access the BBS to
determine the identity of the owner but was unable to do so because its
software was incompatible with the BBS.

Teleconnect states that its actions are not discriminatory to BBSs and states
that it currently provides access to literally hundreds of BBSs around the
country. The report also states that Teleconnect's policy to block when
unauthorized use is detected is employed whether or not such use involves a
BBS. Teleconnect advises that when an investigation is concluded or when a
complaint is received concerning the blocking, the blocking will be lifted, as
in the case of the Iowa BBS. However, Teleconnect notes that blocking will be
reinstated if illegal "hacking" recurs.

Teleconnect advises that it currently has no ongoing investigations within the
State of Michigan and therefore, is not presently blocking any BBSs in
Michigan. However, Teleconnect states that it is honoring the request of other
carriers and customers to block access to certain numbers.

The Branch has reviewed the file on this case. In accordance with the
Commission's rules for informal complaints it appears that the carrier's report
is responsive to our Notice. Therefore, the Branch, on its own motion, is not
prepared to recommend that the Commission take further action regarding this
matter.

- -

This letter leaves me with a ton of questions. First, let's be fair to
Teleconnect. Long distance carriers are being robbed of hundreds of thousands
of dollars annually by "hackers" and must do something to prevent it. However,
call blocking is NOT going to stop it. The "hacker" still has access to the
carrier network and will simply start calling other numbers until that number,
too, is blocked, then go on to the next. The answer is to identify the
"hacker" and put him out of business. Teleconnect is taking a cheap, quick fix

approach that does nothing to solve the problem, and hurts the phone users as a whole.

They claim that their customers are able to use other networks to complete their calls if the number is being blocked. What if other networks decide to use Teleconnect's approach? You would be forced to not only keep an index of those numbers you call, but also the long distance carrier that will let you call it! Maybe everyone will block that number, then what will you do? What if AT&T decided to block calls? Do they have this right too?

And how do you find out if the number is being blocked? In the case of Mr. Kyhl's BBS, callers were given a recording that stated the number was not in service. It made NO mention that the call was blocked, and the caller would assume the service was disconnect. While trying to investigate why his calls were not going through, Mr. James Schmickley placed several calls to Teleconnect before they finally admitted the calls were being blocked! Only after repeated calls to Teleconnect was the blocking lifted. It should also be noted that Mr. Kyhl's bbs is not a pirate bbs, and has been listed in a major computer magazine as one of the best bbs's in the country.

As mentioned before, MBT will work with the long distance carriers to find these "hackers." I assume that the other local carriers would do the same. I do not understand why Teleconnect could not get help in obtaining Mr. Kyhl's address. It is true the phone company will not give out this information, but WILL contact the customer to inform him that someone needs to contact him about possible fraud involving his phone line. If this policy is not being used, maybe the FCC should look into it.

Call blocking is not restricted to BBSs, according to Teleconnect. They will block any number that reaches a $500 fraud loss. Let's say you ran a computer mail order business and didn't want to invest in a WATS line. Why should an honest businessman be penalized because someone else is breaking the law? It could cost him far more the $500 from loss of sales because of Teleconnect's blocking policy.

Teleconnect also claims that "they are honoring the request of other carriers and customers to block access to certain numbers." Again, MBT also has these rules. But they pertain to blocking numbers to "certain numbers" such as dial-a-porn services, and many 900-numbers. What customer would ever request that Teleconnect block incoming calls to his phone?

And it is an insult to my intelligence for Teleconnect to claim they could not log on to Mr. Kyhl's BBS. Do they mean to say that with hundreds of thousands of dollars in computer equipment, well trained technicians, and easy access to phone lines, that they can't log on to a simple IBM bbs? Meanwhile, here I sit with a $50 Atari 800xl and $30 Atari modem and I have no problem at all accessing Mr. Kyhl's bbs! What's worse, the FCC (the agency in charge of regulating data transmission equipment), bought this line too! Incredible!!!

And finally, I must admit I don't have the faintest idea what Section A.20.a.04 of Teleconnect's Tariff FCC No. 3 states, walk into your local library and ask for this information and you get a blank look from the librarian. I know, I tried! However, MBT also has similar rules in their tariffs. Teleconnect claims that the FCC tariff claims that "service may be refused or disconnected without prior notice by Teleconnect for fraudulent, unauthorized use". This rule, as applied to MBT, pertains ONLY to the subscriber. If an MBT customer were caught illegally using their phone system then MBT has the right to disconnect their service. If a Teleconnect user wishes to call a blocked number, and does so legally, how can Teleconnect refuse use to give them service? This appears to violate the very same tarriff they claim gives them the right to block calls!

I have a few simple answers to these questions. I plan, once again, to send out letters to the appropriate agencies and government representatives, but I doubt they will go anywhere without a mass letter writing campaign from all of you. First, order that long distance companies may not block calls without the consent of the customer being blocked. Every chance should be given to him to assist in identifying the "hacker," and he should not be penalized for other people's crimes. There should also be an agency designated to handle appeals if call blocking is set up on their line. Currently, there is no agency,

public service commission, or government office (except the FCC) that you can
complain to, and from my experience trying to get information on call blocking
I seriously doubt that they will assist the customer.

Next, order the local phone carriers to fully assist and give information to
the long distance companies that will help identify illegal users of their
systems. Finally, order the Secret Service to investigate illegal use of long
distance access codes in the same manner that they investigate credit card
theft. These two crimes go hand in hand. Stiff fines and penalties should be
made mandatory for those caught stealing long distance services.

If you would like further information, or just want to discuss this, I am
available on Genie (G.Cross) and CompuServe (75046,267). Also, you can reach
me on my bbs (FACTS, 313-736-4544). Only with your help can we put a stop to
call blocking before it gets too far out of hand.

>------------=====END=====--------<

                          ==Phrack Inc.==

            Volume Three, Issue 29, File #10 of 12

       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 XXIX/Part 1   PWN
       PWN   PWN
       PWN   November 17, 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

            Welcome to Issue XXIX of Phrack World News!

Although Phrack Inc. is officially four years old, Phrack World News is not.
PWN originally in its first issue (which was in Phrack Inc. II... its a long
story) was known as "Phreak World News," but quickly changed and starting with
Phrack Inc. Issue III became Phrack World News as you see it today.

This issue of Phrack World News contains stories and articles detailing events
and other information concerning AT&T, Clifford Stoll, Kent O'Brien, Kevin
David Mitnick, Datacrime, DEC, FAX, FCC, Galactic Hackers Party, IBM, Lawrence
Livermore National Laboratory, Leonard Mitchell DiCicco, MCI, NASA, Robert
Morris, Shockwave Rider, SummerCon '89, The "NEW" TAP Magazine, 2600 Magazine,
Viruses, Worms Against Nuclear Killers, and much more so keep reading and
enjoy.

:Knight Lightning

        "The Real Future Is Behind You... And It's Only The Beginning!"
_____

Judge Proposes Community Service For Hacker's Accomplice   October 13, 1989
~~~~~~
by Kathy McDonald (New York Times)

LOS ANGELES -- A federal judge says she is inclined to sentence a man who
pleaded guilty to helping computer hacker Kevin Mitnick steal a computer
security program to community service and asked him to submit a proposal on
such a sentence.

U.S. District Judge Mariana R. Pfaelzer said Leonard Mitchell DiCicco, of
unincorporated suburban Calabasas, had been helpful in the case, in which he
reported Mitnick to officers at Digital Equipment Corporation in Massachusetts.

Mitnick has admitted he stole a DEC computer security program and
electronically brought it to California.

Pfaelzer gave DiCicco, age 23, until November 1 to come up with a detailed
proposal for his community service.

"I favor the handicapped, older people, something which is out in the
community," Pfaelzer said.

DiCicco pleaded guilty in July to one count of aiding and abetting the
interstate transportation of stolen property. He admitted that in 1987 he let
Mitnick, age 25, of suburban Panorama City, use his office computer at
Voluntary Plan Administrators in Calabasas to break into the DEC system.

Mitnick pleaded guilty and was sentenced in July to one year in prison and six
months in a community treatment program aimed at breaking his "addiction" to
computer hacking.

Under a plea agreement with the government, DiCicco pleaded guilty in exchange

for a promise that he would not be prosecuted for any of the other instances of computer hacking he and Mitnick carried out.

He said after Thursday's (October 12) court appearance that he would like to put his computer talents to use to help others.

Assistant U.S. Attorney James Asperger did not object to giving DiCicco community service rather than a prison term, saying: "I think Mr. DiCicco's cooperation in this case was essential to the prosecution of both Mr. Mitnick and himself. He is certainly lower in culpability than Mr. Mitnick."

- -

If you are looking for other articles related to Leonard Mitchell DiCicco and the famous Kevin David Mitnick please refer to;

"Pacific Bell Means Business"   (10/06/88) PWN XXI....Part 1
"Dangerous Hacker Is Captured"   (No Date) PWN XXII...Part 1
"Ex-Computer Whiz Kid Held On New Fraud Counts" (12/16/88) PWN XXII...Part 1
"Dangerous Keyboard Artist"   (12/20/88) PWN XXII...Part 1
"Armed With A Keyboard And Considered Dangerous" (12/28/88) PWN XXIII..Part 1
"Dark Side Hacker Seen As Electronic Terrorist" (01/08/89) PWN XXIII..Part 1
"Mitnick Plea Bargains"   (03/16/89) PWN XXV....Part 1
"Mitnick Plea Bargain Rejected As Too Lenient"   (04/25/89) PWN XXVII..Part 1
"Computer Hacker Working On Another Plea Bargain" (05/06/89) PWN XXVII..Part 1
"Mitnick Update"   (05/10/89) PWN XXVII..Part 1
"Kenneth Siani Speaks Out About Kevin Mitnick"   (05/23/89) PWN XXVII..Part 1
"Judge Suggests Computer Hacker Undergo Counseling"(07/17/89) PWN XXVIII.Part 1
"Authorities Backed Away From Original Allegations"(07/23/89) PWN XXVIII.Part 1

How Hacker Jammed 911 Police Lines   October 4, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

by Benny Evangelista

He is a brilliant, but lonely teenage computer hacker with too much time on his hands.

And the police said the 16-year-old San Gabriel boy used that time to put a sophisticated high-tech spin on age-old teenage telephone pranks by tying up police emergency lines from Hayward, California to Cedar Rapids, Iowa, and harassing other people, all from what he thought was the safety of his home Commodore 64 computer.

The calls that jammed Hayward police and Alameda County sheriff's lines were potentially dangerous, but officials said that no emergency was neglected because of them.

This is the way he got his kicks, but he had most of us just absolutely crazed," said Connie Bullock, security director for one of the long-distance companies that suffered thousands of dollars of losses.

The boy, who police would not identify because of his age, is <was> scheduled to be arraigned October 16th in Los Angeles County Juvenile Court for making telephone bomb threats, fraudulently obtaining long-distance telephone service, interfering with a police officer and making harassing phone calls.

"Our goal is to get him on probation so we can doctor him for the next couple of years," said Sgt. Bernie Kammer, of the Los Angeles County sheriff's computer crime detail.

"Hopefully, he may be one of the guys who sends the next space capsule up," Kammer said.

The hacker, who has used handles like "Kent O'Brien," surfaced sometime last October, said Bullock, director of network security for ComSystems Incorporated, a Van Nuys-based long distance company.

Bullock learned that someone had tapped into the electronic phone mail system of a Cedar Rapids-based long-distance company using ComSystems lines.

A security officer for the Iowa company began receiving harassing and threatening calls, some at home in the middle of the night, she said.

The hacker became good at cracking home answering-machine codes in the Southern California area and possibly elsewhere, and changed several outgoing messages, she said.

He also broke into the phone mail system at Sears administrative office in Hayward, California and called workers there, she said. He even commandeered one phone mail box and had other people leave messages.

He would also make anonymous calls or just let the phone ring in the middle of the night and hang up. He phoned in bomb threats to his old high school and a fast-food restaurant, Kammer said.

In all cases, he used a computer synthesizer to disguise his voice, Kammer said. And he routed the calls in ways to make tracing impossible.

Then he started calling Cedar Rapids police emergency 911 lines, bombarding dispatchers in the middle of the night with a series of computer-assisted calls that would tie up the lines for hours. He would make small talk and ask about the weather, said Cedar Rapids Detective Stan McCurg.

The boy could call up five or six other people, hold their lines captive and route the calls to police, McCurg said.

"The scary thing is he had the capability to screw you over and you couldn't do anything about it," McCurg said.

Police say the boy pulled the same trick on the Alameda County Sheriff's office, San Francisco police and the Los Angeles County sheriff's office in Crescrenta Valley.

The calls did not cause any safety problems, but there was always that potential, Kammer said.

The big break came after the boy started calling Hayward police dispatchers in late February. At first, the dispatchers played along, trying to find out who and where the boy was while the boy gave false clues to throw them off.

"It was like, 'Catch me if you can,'" said Hayward Detective Dennis Kutsuris.

On March 2, dispatchers kept him talking from 8:10 a.m. to 1:20 p.m., long enough to trace the call to his San Gabriel home. That night, police served a search warrant and found the boy in bed talking on the phone using his synthesizer.

The hacker was a lonely boy who dropped out of high school because it didn't challenge him, but had passed his general education equivalency exam and was taking courses from a community college, according to Kammer and Bullock.

Police seized the computer equipment, but formal charges were not filed until last month because of the complex followup investigation, Kammer said.

Bullock said her company lost about $71,000 worth of calls, plus four angered customers. Kammer said although police believe the loss could be "hundreds of thousands" of dollars, they can only prove the loss of $2000 in court.

In the meantime, Hayward police received another call September 6th from a computer-synthesized voice that they feel came from the boy. Kammer said a relative had given the boy another computer, but they have no proof that he was back to his old tricks.

Still, that incident, along with Cedar Rapids police reports will be used for a probation report, Kammer said.

Bullock said the case was intriguing at first, but became frustrating as her file grew to 2 feet thick.

"He had me by the guts," she said. "I was obsessed with finding him. He's a typical 16-year old, but a little more menacing. He is pretty smart, but he had absolutely nothing to do, but sit in his room with his computer equipment and all he had to do was talk on the phone."

_____

Just The FAX, Please   November 6, 1989
~~~~~~~~~~~~~~~~~~~~

by Noam Cohen (New York Times)

Teachers in rural Minnesota are ready to hear the most up-to-date version of the oldest excuse in the book: "Honest, teach, the fax ate my homework."

Yes, the facsimile machine has gone to school in Sibley County, an agricultural area 60 miles southwest of Minneapolis-St. Paul.

It is the last component to be installed in a four-year-old interactive television system, or ITV, that brings advanced classroom instruction to small, isolated areas through closed-circuit cable television.

In an education system where students adjust the contrast knobs to get a better look at their calculus teacher, it is hardly surprising that these students are the first in the country to use the fax to receive or hand in homework.

David Czech, the telecommunications director for the school district who is responsible for its cable system education program, said that now, televised teachers can even give surprise quizzes.

"The fax makes the classroom truly self-contained," said Kelly Smith, an assistant principal at Gibbon-Fairfax-Winthrop High School, in Sibley County, who taught mathematics for the ITV program before fax machines were introduced. He said that when he taught he "had to rely on transportation in the district and assignments always stacked up."

The fax machines, part of a special line made by Ricoh Corporation, transmit on the same wiring that carries the television image to students. By using cable instead of telephones, the district saves money on telephone costs and receives quicker, cleaner copies.

The machines have a built-in copier, allowing one student to retrieve the assignment and hand copies to classmates (usually no more than eight). Students then use the machine to hand back work.

The Sibley County school district purchased and installed the fax machines with the remaining $22,000 of a $150,000 state grant for ITV, according to Czech.

The machines, which school officials and a Ricoh spokeswoman say are the first to be used in high school education, have generated interest elsewhere. Czech says he has received calls from education officials in Hawaii, Wisconsin, Ohio and other parts of Minnesota.

_____

MCI Sues AT&T -- Charges Deceptive Advertising   October 12, 1989
~~~~~~
        "We Welcome The Opportunity To Discuss Who Is Misleading Whom..."

AT&T is using false and malicious advertising to protect its long-distance business, MCI Communications Corporation charges in a lawsuit filed Tuesday, October 10.

MCI, whose 10 percent market share makes it a distant number two to AT&T's 75 percent, says its giant rival is resorting to false claims in the hope of stemming the loss of 100,000 customers to MCI each week.

AT&T, however, says it will defend itself with a countersuit. According to AT&T spokesman Herb Linnen: "We welcome the opportunity to discuss who is misleading whom... we have been quite concerned for some time now about MCI's misleading print and broadcast advertising. We have taken our complaints directly to MCI without success."

He added, "AT&T stands behind its advertising."

This latest litigation is simply the latest chapter in MCI's long and very
bitter battle with AT&T, which began in the 1970's when MCI successfully broke
AT&T's long-distance monopoly by offering "Execunet," the first long-distance
service bypassing AT&T offered to the public. The two companies have battled
each other at the Federal Communications Commission, which authorizes the rates
for each, ever since. This is the first time since AT&T's divestiture that the
arguments have been taken into a courtroom.

In an interview, MCI Chairman William McGowan said that "AT&T ads are sleazy,"
and he noted that the nine month old campaign grew increasingly negative,
forcing MCI into the courts.

AT&T responded saying that MCI is resorting to the courts since "...they just
can't hack it in the marketplace..."

McGowan responded that he believes a lawsuit is the only way to fight a company
which is spending two million dollars a day on advertising. He said, "Our
budget is big -- $51 million -- but how do you compete with someone who is nine
or ten times your size in advertising?"

MCI is still studying the impact of the latest round of AT&T ads, but McGowan
said he is sure MCI should have gained "a lot more" than 100,000 customers per
week if not for the advertising. The advertising has not affected professional
telecommunications managers, but does have an impact on individual and small
business customers, he said.

The MCI suit, filed in U.S. District Court in Washington, DC, alleges that
AT&T's advertising campaign "maliciously attacked MCI's honesty and the value
of MCI's products and service by falsely and deceptively representing that it
is superior to its competitors in general, and MCI in particular, in terms of
trustworthiness, quality and price.

MCI's suit cites AT&T ads that assert MCI's rates are cheaper than AT&T's only
when calls are made over 900 miles away and after 7 p.m. MCI's suit also takes
umbrage at AT&T's advertisement which states that MCI customers "might have
better luck calling Mars than trying to reach MCI representatives for an
explanation of their bills."

The ads, the suit charges, also claim non-AT&T companies provide slow telephone
connections; that other companies do not operate worldwide like AT&T; and that
competing 800, facsimile and WATS services are inferior.

The suit says AT&T "has wrongfully profited and MCI has been damaged by being
wrongfully thwarted from maximizing its sales potential."

The suit asks the court to order AT&T to discontinue advertising its services
for a period of one year and that advertisements after that time be approved by
the court and carry a notice to that effect in the advertisement itself.
Additionally, it asks for profits "wrongfully amassed" by AT&T on the sale of
its products and services during the past year, plus interest and legal fees.

McGowan was particularly irked by a claim that MCI's fax service has 57 percent
more problems than AT&T faxes. He said that number was arrived at by figuring
the difference between AT&T service -- with 4.9 percent errors -- and MCI, with
7.7 percent errors. Rather than reporting the 2.8 percent difference, the ad
claims a 57 percent higher rate -- the percentage increase between 4.9 percent
and 7.7 percent.

"Talk about misleading," McGowan said.

"Yes, talk about misleading," said Herb Linnen. "They've survived this long in
part based on the deceptions they've used on a public not well educated on the
technical aspects of telephony... we'll clear this up once and for all in court
with a countersuit."

- -

Unleashing Ma Bell   October 24, 1989

~~~~~~~~~~~~~~~~~~~
by Peter Passell (New York Times)

                    Could AT&T's rivals in long-distance phone
                    service survive no-holds-barred competition?

Since the breakup of the telephone monopoly in 1984, the Federal Communications
Commission has kept AT&T on a short leash to prevent the giant company from
chewing up the "small fry."

But now two of those small fry have grown into profitable multibillion-dollar
corporations, and AT&T is asking the regulators for the freedom to fight for
market share. If the FCC agrees -- a crucial decision could come as early as
Thursday -- high-volume telephone users are likely to reap a bonanza from lower
prices.

When the Bell System was dismembered, analysts generally agreed that rivals
would need a lot of help from Washington to gain a secure foothold in the
long-distance market dominated by the ultimate name-brand company.

The analysts were right: After AT&T's competitors lost their discounts on
regulated charges for hookups to local telephone exchanges, all of them took a
financial bath and some went broke.

But in the ensuing consolidation, a few companies emerged with both the
technical capacity to match AT&T's service and the marketing savvy to sell
themselves to once-skeptical consumers.

MCI Communications now has 12 percent of the long-distance market and in the
last year has grown four times as fast as AT&T.

US Sprint Communications, with its much-ballyhooed all-fiber-optic system, has
an 8 percent share and is the principal carrier for 117 of America's 800
largest companies.

Joel Gross, a communications analyst at Donaldson, Lufkin & Jenrette, believes
a fourth network, assembled from a half-dozen smaller companies, will soon
emerge.

One reason AT&T's rivals have managed to do so well in the last few years is
continuing regulatory discrimination.

Last summer, the FCC switched AT&T from traditional fair-rate-of-return
regulation to a more flexible "price-cap" system that gives the company
discretion to adjust individual rates within a narrow price band.

But neither the old price regulations nor the new ones apply to MCI, US Sprint
and other smaller long-distance companies. And they have taken advantage of
AT&T's inability to cut prices, offering volume discounts where AT&T is most
vulnerable to customer defections.

AT&T has fought back, convincing the FCC to allow it fast-track approval for
rate concessions needed to hang onto its biggest customers.

And it is now asking the commission for broad discretion to cut rates by more
than the 5 percent permitted under the price-cap rule. If the FCC agrees, it
is a sure bet that AT&T will price aggressively, accepting sharp reductions in
its fat profit margins to check its loss of market share.

It is obvious why MCI and US Sprint are unhappy at the prospect of an AT&T
unleashed. But it is not so easy to see how the public would lose from the
ensuing donnybrook.

One worry is that AT&T would slash prices by enough to drive rivals out of
business, and then be free to price-gouge.

But as Peter Pitsch, a former FCC staff member who now consults for AT&T points
out, such "predatory" pricing is only a plausible option if the predator can
hope to make up the inevitable short-term losses with long-term monopoly gains.
And two considerations make such a calculation unlikely.

Once the cables have been laid and the switches installed, it costs very little
to operate a long-distance phone system. Thus even if AT&T were able to drive
MCI and US Sprint into bankruptcy, their creditors would find it advantageous
to continue to sell long-distance services.

And if AT&T somehow did manage to shut down its rivals, the FCC would hardly be
likely to reward it with permission to charge monopoly prices.

Another concern is that price-cutting would make long-distance service
unprofitable for all, discouraging further investment.

That, however, might not be such a bad thing. Losses are capitalism's way of
telling businesses to slow down: There is enormous overcapacity in
long-distance communications and more investment anytime soon is unlikely to be
productive.

Does all this mean the commission will hang tough and permit AT&T to flex its
competitive muscles? A year ago, when the FCC was dominated by Reagan-appointed
free marketers, the answer would have been easy.

Today, with a Bush-appointed majority led by a chairman, Alfred Sikes, of less
certain ideological bent, it is hard to say.

MCI and US Sprint have managed to squeeze a lot of regulatory mileage out of
their underdog status, and certainly will not give up the privileges that go
along without a fight.

- -

AT&T Strikes Back: Countersues MCI   October 27, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
AT&T struck back on Thursday, October 27 at advertising claims made by MCI
Communications Corporation and received two rulings from the Federal
Communications Commission affecting regulation of its long distance services.

AT&T said in a countersuit against MCI filed in Washington, DC that MCI was
misleading consumers through false and deceptive advertising in its business
and residential long distance service. AT&T's filing denied similar
allegations made by MCI in a suit filed October 10.

Victor Pelson, AT&T group executive, said MCI unfairly compared its discount
service with AT&T's regular long distance service rather than its discount
service. Pelson also denied claims that the quality of MCI voice service was
superior to AT&T's, or that its facsimile service featured fewer garbled
transmissions than AT&T's.

"We intend to clarify any misconceptions in the market," said Merrill Tutton,
AT&T Vice President for consumer marketing.

MCI spokeswoman Kathleen Keegan Thursday responded that, "our ad claims are
accurate... We will soon be filing a motion for a preliminary injunction to
cause AT&T to cease its advertising campaign."

Also on Thursday, the Federal Communications Commission upheld a decision
giving AT&T greater freedom to compete for big corporate customers but rejected
another pricing plan by AT&T.

The FCC voted unanimously to uphold a pricing plan known as Tariff 12, which
lets AT&T offer corporate customers a package of communications services. AT&T
contends it is at a disadvantage because MCI does not have to submit detailed
filings to the FCC before they can serve customers. MCI had challenged Tariff
12, asking the FCC to overrule it and prohibit AT&T from offering full service
communications packages to its customers.

In the second item, the FCC declared unlawful a pricing plan known as Tariff
15, that AT&T had applied solely to a single customer, the Holiday Corporation,
owner of the largest hotel chain in the United States. The FCC said AT&T could
no longer justify the special rates to a single customer to meet competition
when MCI was making the same service available to customers generally.

>------------=====END=====---------<

```
                          ==Phrack Inc.==

                 Volume Three, Issue 29, File #11 of 12

          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 XXIX/Part 2           PWN
          PWN                                             PWN
          PWN                 November 17, 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
```

Offensive Message Flashes At Busy City Corner   October 25, 1989
~~~~~~
by Linda Wheeler (Washington Post)

An offensive message that mystified the owners of an electronic information
board was flashed Monday, October 23 at Connecticut Avenue and L Street NW, one
of the city's (Washington DC) busiest intersections.

A Georgetown University law student, Craig Dean, said he saw the message;

          "HELP STAMP OUT A.I.D.S. NOW: KILL ALL QUEERS AND JUNKIES"

It flashed five times in 25 minutes. Minutes after seeing the message, he
called the city Human Rights Office and the Washington Blade, a gay community
newspaper.

Doug Hinckle, a staff photographer for the Blade, saw the message flash once
and photographed it.

Judith Miller, president of Miller Companies, which own the building at 1101
Connecticut Avenue NW and the message board, said she did not know how the
statement got onto the board. She refused to believe it had appeared until she
was shown of the photographs.

Her company has complete control of the board and does not accept any paid
messages or advertisements, Miller said. "I would never do anything like
that," she said. "There is no way I would allow such a statement to appear."

Yesterday, Keller, a five-year employee of the Miller Companies, said he did
not write the statement and does now know how it became part of the normal flow
of headline news.

Miller said she believes her computer system may have a "virus" and will have
experts search to find where the unauthorized statement originated. "How
absolutely awful," she said of the message.
_____

"WANK" Worm On SPAN Network   October 17, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
>From The Computer Emergency Response Team

On October 16, the CERT received word from SPAN network control that a worm was
attacking SPAN VAX/VMS systems. This worm affects only DEC VMS systems and is
propagated via DECnet protocols, not TCP/IP protocols. If a VMS system had
other network connections, the worm was not programmed to take advantage of
those connections. The worm is very similar to last year's HI.COM (or Father
Christmas) worm.

This is NOT A PRANK. Serious security holes are left open by this worm. The
worm takes advantage of poor password management, modifies .com files, creates
a new account, and spreads to other systems via DECnet.

It is also important to understand that someone in the future could launch this
worm on any DECnet based network. Many copies of the virus have been mailed
around. Anyone running a DECnet network should be warned.

R. Kevin Oberman from Lawrence Livermore National Labs reports:

    "This is a mean bug to kill and could have done a lot of damage.
    Since it notifies (by mail) someone of each successful penetration
    and leaves a trapdoor (the FIELD account), just killing the bug is
    not adequate. You must go in an make sure all accounts have
    passwords and that the passwords are not the same as the account
    name."

The CERT/CC also suggests checking every .com file on the system. The worm
appends code to .com files which will reopen a security hole everytime the
program is executed.

An analysis of the worm appears below and is provided by R. Kevin Oberman of
Lawrence Livermore National Laboratory. Included with the analysis is a DCL
program that will block the current version of the worm. At least two versions
of this worm exist and more may be created. This program should give you
enough time to close up obvious security holes.

- -

                        Report on the W.COM worm.
                            R. Kevin Oberman
                          Engineering Department
                   Lawrence Livermore National Laboratory
                            October 16, 1989

The following describes the action of the W.COM worm (currently based on the
examination of the first two incarnations). The replication technique causes
the code to be modified slightly which indicates the source of the attack and
learned information.

All analysis was done with more haste than I care for, but I believe I have all
of the basic facts correct.

Here is a description of the program:

1. The program assures that it is working in a directory to which the owner
   (itself) has full access (Read, Write,Execute, and Delete).

2. The program checks to see if another copy is still running. It looks for a
   process with the first 5 characters of "NETW_". If such is found, it
   deletes itself (the file) and stops its process.

   Note: A quick check for infection is to look for a process name starting
          with "NETW_". This may be done with a SHOW PROCESS command.

3. The program then changes the default DECNET account password to a random
   string of at least 12 characters.

4. Information on the password used to access the system is mailed to the user
   GEMPAK on SPAN node 6.59. Some versions may have a different address.

5. The process changes its name to "NETW_" followed by a random number.

6. It then checks to see if it has SYSNAM priv. If so, it defines the system
   announcement message to be the banner in the program:

        W O R M S   A G A I N S T   N U C L E A R   K I L L E R S
      _____
      __ _____ _____ _____ _____ _____ __ _____/
       \ \ \   /\   / /   / /\ \ | \ \ \| | || / /   /
        \ \ \ / \ / /   / /__\ \ | |\ \ | | ||/ /   /
         \ \ \/ /\ \/ /   / _____ \ | | \ \| | ||\ \   /
          _\ /__\ /____/ /_____\ ____| |__\| |____| |_\ _/
           _____/

```
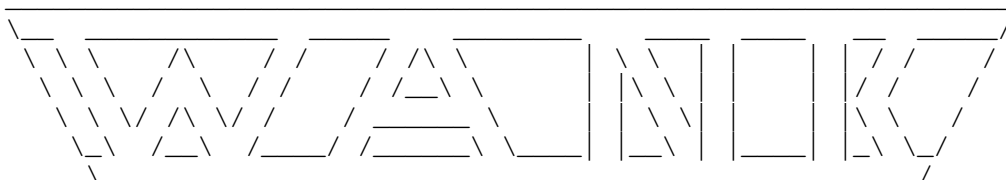    \                                                         /
     \      Your System Has Been Officially WANKed      /
      _____/
```

         You talk of times of peace for all, and then prepare for war.

7. If it has SYSPRV, it disables mail to the SYSTEM account.

8. If it has SYSPRV, it modifies the system login command procedure to
   APPEAR to delete all of a user's file. (It really does nothing.)

9. The program then scans the accounts logical name table for command
   procedures and tries to modify the FIELD account to a known password with
   login form any source and all privs. This is a primitive virus, but very
   effective IF it should get into a privileged account.

10. It proceeds to attempt to access other systems by picking node numbers at
    random. It then used PHONE to get a list of active users on the remote
    system. It proceeds to irritate them by using PHONE to ring them.

11. The program then tries to access the RIGHTSLIST file and attempts to access
    some remote system using the users found and a list of "standard" users
    included with the worm. It looks for passwords which are the same as that
    of the account or are blank. It records all such accounts.

12. It looks for an account that has access to SYSUAF.DAT.

13. If a priv. account is found, the program is copied to that account and
    started. If no priv account was found, it is copied to other accounts
    found on the random system.

14. As soon as it finishes with a system, it picks another random system and
    repeats (forever).

- -

Computer Network At NASA Attacked By Rogue Program   October 18, 1989
~~~~~~
by John Markoff (New York Times)

A rogue computer program attacked a worldwide network of the National
Aeronautics and Space Administration on Monday, October 16, inflicting no
damage but forcing officials to disconnect the network from sensitive military
and space systems.

Security experts speculated that the program was written by someone who opposed
Tuesday's (October 17) scheduled launching of the space shuttle Atlantis, which
was to carry a nuclear-powered satellite into orbit. The launching was
postponed because of bad weather.

NASA officials said the rogue program attacked an academic and research
network, the Space Physics Analysis Network, which is not used for space
shuttle mission control.

But a NASA official said the agency felt compelled to disconnect several links
between the network and an operational space shuttle network as a precaution.

Computer security experts at several national laboratories said the Department
of Defense had also severed the connection between commercial and research
networks and nonclassified network that connects United States military
installations and contractors around the world.

The program was designed to copy itself secretly and send unwanted, sometimes
vulgar messages to users of the NASA network. It also tricks users into
thinking that data have been destroyed, although no data are damaged.

Like similar programs that have been sent into computer networks by pranksters
and saboteurs, it exploited a flaw in the security system designed to protect
the computers on the network.

Computer security experts said Tuesday that they knew of about 60 computers that had been affected by the program. A NASA spokesman said the program was still spreading.

While the network is widely available to academic researchers with personal computers, the rogue program was designed to attack only 6,000 computers manufactured by the Digital Equipment Corporation.

The flaw in the security of the Digital Equipment computers had been widely publicized over a year ago even before a similar rogue program jammed a group of interconnected international networks known as the Internet. NASA officials said the program was only able to attack computers in which the necessary steps had not been taken to correct the flaw.

Among the messages the program displayed on all infected computers was one that read: "Worms Against Nuclear Killers. You talk of times of peace for all, and then prepare for war."

Computer scientists call this kind of program a worm, a reference to a program first described in the novel "Shockwave Rider" by a science fiction writer, John Brunner.

_____

Virus Controversies Again   October 6, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~
by John Markoff (New York Times)

        "The issue has also sparked interest among computer scientists."

Harold Highland, editor of Computers & Security, a professional journal, said he had received two research papers describing how to create such anti-virus programs.

He has not decided whether to publish them.

"No one has raised the obvious ethical questions," he added. "I would hate to see a virus released to fight viruses. Until it's tested you don't know whether it's going to do more damage than the program it is designed to fight."

A number of these programs have already been written, computer researchers said.

The one that destroyed the data on business and governmental personal computers in the United States was reportedly designed by a Venezuelan programmer. How many computers were affected and where they were is unclear.

That program is called Den Zuk, or Search. It was intended to attack a destructive program known as the Brain Virus that was distributed in 1986 by two brothers who owned a small computer store in Pakistan.

Errors in the design of the program illustrate the potential danger of such viruses, critics say. Fridrik Skulason, a microcomputer specialist at the University of Iceland in Reykjavik, who has disassembled the program, said the author of Den Zuk had failed to take into account the different capacities of disks available for IBM and IBM-compatible machines.

Because of that simple error, when the program infects a higher-capacity disk it destroys data.

"They probably wrote with good intention," he said. "The only problem is that the programmers were not able to do their job correctly."

At least two other anti-viral viruses have already been devised, said Russell Brand, a computer security researcher at Lawrence Livermore.

He said programmers at one company, which he would not identify, had written the programs to combat the Scores virus, a program that infected Macintosh computers last year.

He added that even though the programs were designed so they could not go

beyond the company's own computers, there had been a heated debate over whether
to deploy the programs. He said he did not know how it was decided.

Brand said a group of computer researchers he works with at Lawrence Livermore
had written several self-replicating programs after the appearance of the rogue
program that Morris of Cornell is accused of writing. But he added that the
group had never given permission to release the programs.

The debate over vigilante viruses is part of a broader discussion now taking
place among some computer researchers and programmers over what is being termed
"forbidden knowledge."

"There are ethical questions any time you send something out there that may
find itself invited on to somebody else's computer," said Pamela Kane, author
of a book on computer virus protection.

In California this month a group of computer hackers plans to hold a forum on
"forbidden knowledge in a technological society."

While the role of the computer hacker has been viewed as mischievous in a
negative way, hackers have consistently played a role as innovators, said Lee
Felsenstein, a Berkeley, California, computer expert who designed several early
personal computers.

"Computer hacking was originally a response to the perception of a priesthood's
control over immensely powerful technological resources," he said. "Informed
individuals were able to break the power of this priesthood through gaining and
spreading the body of forbidden knowledge."

- -

Dreaded Personal Computer Virus May Be Only A Cold   October 6, 1989
~~~~~~

by Don Clark (New York Times)

It won't be much of a plague. But the hysteria anticipating it has been
world-class.

Those observations come from computer-security experts as they await Datacrime,
a virus program set to attack IBM-compatible personal computers starting
Thursday, October 12, 1989.

Analyses of the program, also called the Columbus Day Virus, show that it is
indeed destructive. It just hasn't spread very far.

"It's going to be the week of the non-event," predicted John McAfee, a Santa
Clara, California, consultant who serves as chairman of the Computer Virus
Industry Association. "You have more chance of being hit by a meteor than
getting this virus."

McAfee Associates, which acts as a clearinghouse for virus information, has
received just seven confirmed reports of Datacrime in six months -- compared
with three to 50 reports per day about another virus that originated in Israel
in 1987. He thinks only 50 copies of Datacrime exist, and 40 of those are in
the hands of researchers.

"It's gotten more publicity than it deserves," agreed Russell Brand, another
virus expert, who advises Lawrence Livermore National Laboratory.

Brand expects to find just 20 copies among the 75,000 computers he monitors at
1,000 sites.

Such projections are disputed by some. They are based on how often Datacrime
has been detected by computer users using special software that scans their
systems for the virus.

The virus could have infected many users who have not bothered to scan their
systems, McAfee concedes.

Fears have been whipped up by the news media and computer managers at companies

and government agencies. Companies promoting products to eradicate viruses
also have played a role -- understandably.

Staid IBM Corporation this week took the unusual step of offering a program
that checks systems for viruses. The company hasn't detected the virus in its
own operations, but concedes that many customers are worried. "They are asking
us how we protect our software-development operations from viruses," said Bill
Vance, who was appointed a year ago as IBM's director of secure systems.

Bank of America, a huge IBM customer with 15,000 PCs, recently put out a
company-wide notice advising users to make backup copies of their computer data
by Wednesday, the day before the virus is programmed to strike.

Three different government agencies have panicked and sent out multiple
versions of incorrect advice," Brand said.

Worried calls have deluged McAfee's office, which has just three lines for
computer communications and three for voice.

"We put the phone down and it's 30 seconds before it rings again," he said.

Computer sleuths detected Datacrime -- and have detected other viruses -- by
looking for changes in the size of data files and in the way programs operate.
The underlying code used to write the program, once disassembled by experts,
indicates when the program will activate itself.

The identity of Datacrime's author isn't known, although some reports have
linked the virus to an anonymous hacker in Austria. It first began showing up
in March, McAfee said, and gained notoriety after it was discussed at the
midsummer Galactic Hackers Conference in Amsterdam.

It appears to be relatively prevalent in the Netherlands and other European
countries. Dutch computer users have reportedly bought hundreds of programs
that are said to detect and destroy the program.

Like other viruses, Datacrime rides along with innocuous programs when they are
exchanged over a computer network or computer bulletin board or through
exchange of infected disks. Unlike many viruses, it has been designed to later
insert itself in data files that users don't often examine.

If one of the programs is executed after the target date, Datacrime proceeds
with its dirty work -- destroying the directory used to keep track of files on
a computer's hard disk. The crime is analogous to destroying a card file in
the library.

"By destroying this one table you can't find where any of your data is," said
Brand.

But no one should really be in a fix if he makes backup copies of data, experts
say. The data, once safely stored on another disk drive or on magnetic tape,
can be restored by computer professionals even if the virus has infected the
backup files.

- -

"Vaccines" To Hunt Down Rogue Programs   October 6, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
by John Markoff (New York Times)

Ever since a rogue program created by a graduate student jammed a nationwide
computer network last year, the rapid spread of such disruptive software, often
known as viruses, has caused growing alarm among computer users.

Now, to fight fire with fire, some companies, individuals and even a government
research laboratory are crafting a new breed of what have been called
anti-viruses to hunt down intruders.

The trouble is, some computer security experts say, the problem of viruses may
be exaggerated -- and the new crime fighter may do even more damage than the
criminal.

Much like an infection, a well-intended but badly designed program to stop
viruses can run amok, knocking out thousands of computers or destroying vast
amounts of data.

Indeed, one of the anti-virus programs intended to defeat a known virus has
already destroyed data on business and governmental personal computers in the
United States.

The issue has touched off a heated debate over whether the creation of these
high-technology vigilantes is a responsible action. "The risks are just
enormous," said Peter Neumann, a computer security expert at SRI International,
a technology research center in Menlo Park, California. "It's an unbelievably
unsafe thing to do."

But Chris Traynor, a programmer at Divine Axis, a software development company
in Yonkers, New York, argues that anti-virus programs can be contained so that
they do not spread out of control, reaching and possibly damaging data in other
computers. His company is now trying to design such a program.

Computer researchers at the Lawrence Livermore Laboratory, a federal weapons
center in Livermore, California, have designed similar programs that patrol
computer networks in search of breaches through which viruses could enter the
system.

Viruses, which got their name because they mimic in the computer world the
behavior of biological viruses, are programs, or sets of instructions, that can
secretly be spread among computers.

Viruses can travel either over a computer network or on an infected disk passed
by hand between computer users.

Once the infection has spread, the virus might do something as benign as
displaying a simple message on a computer screen or as destructive as erasing
the data on an entire disk.

Computer security experts have been concerned for several years by the
emergence of vandals and mischief makers who deliberately plant the destructive
programs.

But in recent weeks international alarm has reached new heights as rumors have
spread that a virus program will destroy data on thousands of computers this
month, on Friday the 13th.

Computer security researchers said the virus, known as Datacrime, was one of at
least three clandestine programs with internal clocks set to destroy data on
that date.

As is usually the case, no one knows who wrote the program, but U.S. military
officials have mentioned as possible suspects a European group linked to West
German terrorists and a Norwegian group displeased with the fame of Christopher
Columbus, who is honored next week.

Largely in response to customer concerns, IBM said on Monday that it was
offering programs for its personal computers that would scan for viruses.

But several computer security experts say public fears are largely exaggerated.

They note that there have been fewer than a dozen reported appearances of the
Datacrime virus in the United States, and contend that the whole issue is
overblown.

Still, in the personal computer world, where many users have little knowledge
of the technical workings of their machines, concern over computer viruses has
become widespread.

The issue got the most attention last November, when, it is charged, Robert
Morris, a graduate student at Cornell, unleashed a rogue program that because
of a small programming error, ran wildly out of control, copying itself
hundreds of times on thousands of computers, overloading a national network,

As a result of the mounting concern, a new industry has blossomed offering
users protective programs known as vaccines, or anti-viral software.

These programs either alert users that a virus is attempting to tamper with
their computer or scan a computer disk and erase any rogue program that is
detected.

These conventional programs do not automatically migrate from computer to
computer, but now some experts are exploring fashioning programs that graft the
powers of the vaccines onto viruses in order to pursue and stop them wherever
they go.

Designing and spreading such programs was proposed in August by several people
attending an international gathering of computer hobbyists, or "hackers," in
Amsterdam.

They suggested that it was a good way for members of the computer underground
to make a positive contribution.

But many researchers believe the idea is dangerously flawed because of the
possibility of accidentally doing great damage.

Some computer security researchers worry that writing an infectious program to
stop viruses may be taken as an intellectual challenge by hackers who are well
meaning but do not grasp what problems they could create.

"One of the questions that the hacker community is now addressing is what you
do about young hackers," said Stewart Brand, a writer in Sausalito, California,
who is working on a book on outlaw cultures and high technology.

"They don't have a sense of responsibility; they have a sense of curiosity.
These are deliciously debatable issues, and I don't see them going away."

>------------=====END=============<

The Cuckoo's Egg   October 18, 1989
~~~~~~~~~~~~~~~~~
by By Christopher Lehmann-Haupt (New York Times)

            "Tracking a Spy Through the Maze of Computer Espionage"

It all begins with a 75-cent discrepancy in the computer complex's accounting
system. Clifford Stoll, the new man in the office, is assigned to reconcile
the shortfall.

Although an astronomer by training, Stoll has recently seen his grant money run
dry and so has been transferred from the Keck Observatory at the Lawrence
Berkeley Lab down to the computer center in the basement of the same building.
No wizard at computers, he thinks he can pick things up fast enough to get by.
So he sets out to look for the 75 cents.

He quickly discovers that no glitch in the accounting programs has occurred.
No, what seems to have happened is that an unfamiliar user named Hunter briefly
logged on to the system, burning up 75-cents worth of time. Since there is no
account record for Hunter, Stoll erases him from the system. The problem is
solved, or so it seems.

But almost immediately, an operator from Maryland on the same network that the
Lawrence Berkeley Lab uses complains that someone from Stoll's lab is trying to
break into his computer. When Stoll checks the time of the attempt, he
discovers that the account of someone named Joe Sventek, who is known to be in
England for the year, has been used. So he guesses that the user calling
himself Hunter has somehow activated Sventek's account. But who is this hacker
(as Stoll begins to refer to him), where is he operating from and how is he
getting into the system?

Next Stoll sets up systems to alert him every time the hacker comes on line and
monitor his activities without his being aware of it. He watches as the hacker
tries to lay cuckoo's eggs in the system's nest, by which of course he means
programs for other users to feed -- for instance, a program that could decoy
other users into giving the hacker their secret passwords. He watches as the
hacker invades other computer systems on the networks the Lawrence Berkeley Lab
employs, some of them belonging to military installations and contractors.

The mystery grows. Telephone traces gradually establish that the hacker is not
a local operator, is not on the West Coast and may not even be in North
America. But of the various three-letter organizations that Stoll appeals to
for help -- among them the FBI, the CIA and even the National Security Agency
-- none will investigate, at least in an official capacity.

By now a reader is so wrapped up in Stoll's breezily written account of his
true adventure in "The Cuckoo's Egg: Tracking a Spy Through the Maze of
Computer Espionage" that he is happy to overlook certain drawbacks in the
narrative -- most conspicuously the lack of consistently lucid technical talk
and the author's dithering over whether appealing for help to the likes of the
FBI and CIA is selling out to the enemy, a qualm left over from the 1960s
mentality that still afflicts him and his friends.

The only truly annoying aspect of the book is that an endpaper diagram gives away the location of the computer spy. Readers are advised not to look at the endpapers, which do little but spoil the suspense.

Unfortunately, the narrative, too, eventually helps dissipate the story's tension. The officials who finally take over the hunt from Stoll are so reluctant to tell him what is happening that all the suspense he has created simply evaporates. Even Stoll seems to lose interest in the identity of his mysterious antagonist, judging by the limp and haphazard way he finally does give us the news.

Instead of building his story, he allows himself to be distracted by a banal domestic drama centering on his decision to stop being afraid of emotional commitment and marry the woman he has been living with for seven years. And he continues limply to debate the need of the state to defend the security of communications networks against wanton vandalism, as if there were room for serious discussion of the question.

Still, nothing can expunge the excitement of the first two-thirds of "The Cuckoo's Egg," particularly those moments when the author hears his portable beeper going off and bicycles to his lab to read the latest printout of the hacker's activities.

Nothing can relieve our discouragement at the bureaucratic runaround that Stoll got. Had a million dollars worth of damage occurred? the FBI kept asking him.

"Well, not exactly," he would reply. Then there was nothing the FBI could do.

And so it dishearteningly went, although some points should be conceded. Certain individuals in government agencies were extremely helpful to Stoll.

The entire issue of computer-network security was after all a new and unexplored field. And the agencies that the author was asking for help probably knew more about the security threat than they were willing to tell him.

Finally, nothing can diminish the sense of the strange new world Stoll has evoked in "The Cuckoo's Egg" -- a world in which trust and open communication will determine the quality of the future. Whether such values will prevail will prove a drama of momentous significance. Even if this book finally dissipates that drama, its very presence makes these pages worth dipping into.

Digital's Hip To The Standards Thing   October 10, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
NEW YORK -- During a creative session at a major public relations firm to formulate a new corporate message for Digital Equipment Corporation that reflects the company's new direction promoting and supporting computing industry standards, the shopworn phrase "Digital has it now" was replaced by a new tag line that is more contemporary and tied to DEC's adherence to standards.

                    DECrap by Rapmaster Ken
              "Digital's Hip to the Standards Thing"

            I heard some news just the other day
          It sounded kinda strange and I said, "No way!"
            But I heard it again from another source
          It mighta made sense and I said, "Of course!"

            Now computer biz has a lotta confusion
           'Cause operating systems abound in profusion.
          But there's a whole new wave in data processing
          Now that Digital's hip to the standards thing.

                          (chorus)
            Digital's hip to the standards thing!
            Digital's hip to the standards thing!

                    Way back when a long time ago
                       IBM owned the whole show.
                  But other dudes saw this proprietary mess
                And formed committees to find out what's best.

             Some went their own way and built their own software
          But users were perturbed, "It's just a different nightmare."
                   So they got together to look over the picks
                     Put down their money on good 'ol UNIX

                                (chorus)
                    Digital's hip to the standards thing!
                    Digital's hip to the standards thing!

                   Now Digital always kept their users in mind
                     And pushed VMS as the best of the kind.
                     A lotta folks agreed but kept askin' for
                       UNIX support, "We gotta have more!"

                   Soon DEC saw the light and decided to give
                 UNIX to the masses, (sorta live and let live).
                   So DEC's ridin' the wave ahead of the rest
                On a backplane boogie board on top of the crest.

                   No doubt about it DEC's sprouted its wings
                   'Cause Digital's hip to the standards thing.

                                (chorus)
                    Digital's hip to the standards thing!
                    Digital's hip to the standards thing!

_____

Hacker Publications   November 12, 1989
~~~~~~~~~~~~~~~~~~~~
Here is a general overview of a pair of the more popular hardcopy hacker
magazines.

2600 Magazine: The Hacker Quarterly
Volume Six, Number Three
Autumn, 1989

The cover on this issue features a scene from the Galactic Hackers Convention
that took place in Amsterdam, Switzerland, last August. Although it is not
explicitly stated or implied, it would appear that the comic illustration
portrays the hacker "Shatter" being run over by a bus bearing the label "2600
XPRESS."

The articles featured in this issue include:

The Nynex Strike
Grade "A" Hacking: What Is UAPC? by The Plague
Galactic Hacker Party (GHP)
British Telecom's Guilty Conscience
The Death Of COSMOS?
What's Going On
     - Technological Marvels
             o U.S. Sprint Billing Problems
             o U.S. Sprint Voicecards
             o Other Voiceprints
             o Surveillance
     - Hacker Spies (Chaos Computer Club, KGB Hackers discussed)
     - Nynex Bigotry (Gay And Lesbian Organizations)
     - Dial-It News (Pacific Bell 900 Services)
     - Payphone Choices (AT&T, Sprint, MCI, AOS)
     - Overseas Access (AT&T Calls To Vietnam)
     - News From The U.K.
             o Directory Assistance Operators
             o British Telecom To Buy Tymnet From McDonnel Douglas
             o Chat Lines Banned

- One Less Choice (The Source and Compuserve)
- Privacy? What's That?
        o Bulletin Board User Information
        o Illegal Aliens Database
        o Scotland Yard Database
        o Wiretapping
        o Bell of Pennsylvania (giving out confidential information)
        o Personal Smart Card
- Hackers In Trouble
        o Kevin Mitnick
        o Robert Morris
- Hacker Fun
        o Friday The 13th Virus
        o Speed Limit Alterations
        o Delray Beach Probation Office
- Telco Literature (FON Line Newsletter)
- Calling Card Tutorials
- Another Telco Ripoff (C&P Telephone)
- Technology Marches Back
        o French Computer Mixup
        o New York Telephone Repairman Sent On Wild Goose Chases
- And Finally (Bejing Phone Calls)

The Secrets of 4TEL
Letters
- Moblie Telephone Info
- A Southern ANI
- ROLM Horrors
- A Nagging Question (by The Apple Worm)
- A Request
- Another Request (by THOR <claims the Disk Jockey story was a lie>)
- The Call-Waiting Phone Tap (Alternative Inphormation)
- Interesting Numbers (1-800-EAT-SHIT, 800, 900 numbers)
- UNIX Hacking (Unix security, hacking, TCP/IP)
- Intelligent Payphones
- Retarded Payphones

REMOBS by The Infidel
Gee... GTE Telcos by Silent Switchman and Mr. Ed
Voice Mail Hacking... by Aristotle
Punching Pay Phones by Micro Surgeon/West Coast Phreaks
Touch-Tone Frequencies
2600 Marketplace
Carrier Access Codes
Lair of the INTERNET Worm by Dark OverLord
Timely Telephone Tips (from a Defense Department Phone Book)

There were also plenty of other interesting small articles, pictures, and
stories about hackers, telephones, computers and much more. All in all, this
is the best issue of 2600 Magazine I have read in several issues (despite the
fact that some of the material had appeared in Phrack Inc., LOD/H TJs, and/or
Telecom Digest previously). Let's hope they continue to be as good.

Are you interested in 2600 Magazine?

2600 (ISSN 0749-3851) is published quarterly by 2600 Enterprises Inc.,
7 Strong's Lane, NY 11733. Second class postage permit paid at Setauket, New
York.

Copyright (c) 1989, 2600 Enterprises, Inc.
Yearly subscriptions: U.S. and Canada -- $18 individual, $45 corporate.
Overseas -- $30 individual, $65 corporate.
Back issues available for 1984, 1985, 1986, 1987, 1988 at $25 per year, $30 per
year overseas.

Address all subscription correspondence to:

                    2600 Subscription Department
                         P.O. Box 752
                  Middle Island, New York 11953-0752

                    2600 Office Line: 516-751-2600

                         2600 FAX Line: 516-751-2608

- -

TAP Magazine
Issue 94
1989

The new TAP Magazine is a smaller publication in comparison to 2600. The
"outer" cover of this newsletter was a "warning" from The Predat0r concerning
the nature of the material inside. The true or "inner" cover of the newsletter
had the following:

             The Information You've Requested Of TAP Publishing Society
                  A Unit Of The Technological Advancement Party

                              Presents...

"...a family of people dedicated to the advancement of home computer systems
and electronic technology, the study and duplication of related communication
networks and the subsequent utilization of one's own ingenuity in today's
fast-paced world of creative logic."

The articles in this issue of TAP included:

TAP RAP: News From The TAP Staff by Aristotle
Small Tags Protect Big Stores (continued from TAP 93)
Ozone (concerning American Telephone & Telegraph's plans for 1994)
Telephone Wires In New York In 1890
Mercury Fulminate by Dark OverLord
How To Hack Stamps
Hoffman Worked To Help All Of Mankind
Police Raid 3 Jefferson Homes In Search For Computer Hackers by Calvin Miller
SummerCon '89 by Aristotle (includes a copy of the official SummerCon '89
             poster and button, although an error stating that the poster was
             shown at 1/2 size when in reality, the original was 8 1/2" by
             14").

There were a few other interesting "tid bits" of information scattered
throughout the four loose pages including the new TAP logo (that was made to
resemble CompuTel) and other pictures.

The staff at TAP also included a postcard that contained a reader's survey. It
asked all sorts of questions about how the reader liked certain aspects of the
publication... I found the idea to be potentially productive in improving the
quality of the newsletter all around.

The cost of TAP is rather cheap... it is free. For an issue send a self
addressed stamped envelope to:

                              T.A.P.
                          P.O. Box 20264
                    Louisville, Kentucky 40220-0264

:Knight Lightning
_____

Phrack World News QuickNotes
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
1. 911 Improvement Surcharge in Chicago (October 16, 1989) -- Monday morning,
    October 16, Chicago Mayor Richard M. Daley announced that he would submit
    to the city council a plan to increase city telephone taxes by 95 cents per
    line per month, earmarked for improvements to 911 service. Currently there
    is no such flat charge, simply a percentage tax rate on local telephone
    service.

    Daley's spokespeople commented that 911 service here has been a mess for
    years, and that many of the suburbs charge $1.00 per line per month, so 95
    cents should not be unreasonable. There were no details about what is

currently wrong or about what specific improvements Daley has in mind.
- -
2. Hacker Caught by Caller-ID (October 9, 1989) -- MIS Week reported the
    apprehension of a 15-year old hacker who used his Amiga personal computer
    to tap into two minicomputers at Grumman. The youngster was from
    Levittown, Long Island and stumbled into the computer by using a random
    dialing device attached to his computer. Grumman security was able to
    detect the intrusions, and the computer's recording of the boy's telephone
    number led police to his home.
- -
3. 14-Year-Old Cracks TRW Credit For Major Fraud (October 18, 1989) -- A
    14-year-old Fresno, California boy obtained secret "access codes" to the
    files of TRW Credit from a bboard and used them to pose as a company or
    employer seeking a credit history on an individual whose name he picked
    randomly from the phone book. From the histories, he obtained credit card
    numbers which he then used to charge at least $11,000 in mail-order
    merchandise (shipped to a rented storeroom) and make false applications for
    additional cards. He also shared his findings on computer bulletin boards.

    Police began investigating when TRW noticed an unusual number of credit
    check requests coming from a single source, later found to be the youth's
    home telephone number. The high school freshman, whose name was not
    released, was arrested at his home last week and later released to his
    parents. His computer was confiscated and he faces felony charges that
    amount to theft through the fraudulent use of a computer.

    "Here is a 14-year-old boy with a $200 computer in his bedroom and now he
    has shared his data with countless other hackers all over the nation," said
    Fresno Detective Frank Clark, who investigated the case. "The potential
    (for abuse of the information) is incredible." Excerpts provided by
    Jennifer Warren (Los Angeles Times)
- -
4. Computer Virus Countermeasures Article (October 25, 1989) -- Readers of
    Phrack Inc. might be interested in an interesting article in the October
    1989 issue of DEFENSE ELECTRONICS, page 75, entitled "Computer Virus
    Countermeasures -- A New Type Of Electronic Warfare," by Dr. Myron L.
    Cramer and Stephen R. Pratt.
- -
5. Computer Viruses Attack China (November 6, 1989) -- The Ministry of Public
    Safety of People's Republic of China found this summer that one tenth of
    the computers in China had been contaminated by three types of computer
    virus: "Small Ball," "Marijuana," and "Shell." The most serious damage
    was found in the National Statistical System, in which "Small Ball" spread
    in 21 provinces. In Wuhan University, viruses were found in *ALL* personal
    computers.

    In China, three hundred thousand computers (including personal computers)
    are in operation. Due to a premature law system the reproduction of
    software is not regulated, so that computer viruses can easily be
    propagated. Ministry of Public Safety now provides "vaccines" against
    them. Fortunately, those viruses did not give fatal damage to data.
- -
6. More Phone-Card Fraud (October 31, 1989) -- Two men were convicted by Tokyo
    District Court on Monday, October 30, for tampering with Nippon Telephone
    and Telegraph calling cards to increase the number of calls they could
    make. The court ruled that they violated the Securities Transaction Law.

    One man, Kawai, was sentenced to 30 months in prison, and another, Sakaki,
    was given an 18-month suspended sentence.

    Two presiding judges ruled that using falsified telephone cards in pay
    phones is tantamount to using securities.

    However, another judge ruled in a separate case last September that
    tampering with a telephone card does not constitute use of a security, so
    legal observers say it will be up to the Supreme Court.

    According to this most recent s ruling, Kawai changed about 1,600 telephone
    cards, each good for 500-yen worth of telephone calls, into cards worth
    20,000 yen. He sold the altered cards to acquaintances for as much as

3,500 yen.

Sakaki also sold about 320 tampered cards for about 2 million yen.

One of the presiding judges ruled that using tampered telephone cards on
public telephones is the same as misleading Nippon Telegraph and
Telephone Corporation into believing the cards -- false securities -- were
genuine. Taken from The Japan Times

- -

7. Computer Virus Hits Japanese Quake Data (October 30, 1989) -- Tokyo; A
    computer virus has destroyed information at the University of Tokyo's
    seismological and ocean research institutes, a university official and
    local reports said yesterday.

    An official of the university's Ocean Reasearch Institute said the virus
    was detected earlier this month in five of the center's 100 computers,
    but was believed to have first infected the computers in September.

    The virus was found only in personal computers being used by researchers
    and not major computer systems, the official said, requesting anonymity.
    He said the damage was not serious.

    He declined to discuss further details, but a report by the Japan
    Broadcasting Corporation said a virus had also been found in the computers
    at the university's Earthquake Research Institute. Thanks to Associated
    Press news services. (Related article follows)

- -

8. First Virus Attack On Macintoshes In Japan (November 7, 1989) -- Six Macs
    in University of Tokyo, Japan, were found to have caught viruses. Since
    Since this September, Professor K. Tamaki, Ocean Research Institute,
    University of Tokyo, has noticed malfunctions on the screen. In October,
    he applied vaccines "Interferon" and "Virus Clinic" to find his four
    Macintoshes were contaminated by computer viruses, "N Virus" type A and
    type B. He then found ten softwares were also infected by viruses. A
    Macintosh of J. Kasahara, Earthquake Research Institute, University of
    Tokyo, was also found to be contaminated by N Virus and Score Virus. These
    are the first reports of real viruses in Japan.

    Later it was reported that four Macintoshes in Geological Survey of Japan,
    in Tsukuba, were infected by N Virus Type A. This virus was sent from
    United States together with an editor.

- -

9. Hackers Can Tap Into Free Trip (October 1989) -- Attention Hackers: Here
    is your chance to break into a computer system and walk away with a grand
    prize. The "hacker challenge" dares any hacker to retrieve a secret
    message stored in a KPMG Peat Marwick computer in Atlanta.

    This challenge is being sponsored by LeeMah DataCom Security Corporation, a
    Hayward, California, consulting firm that helps companies boost computer
    security. The winner gets an all-expense paid trip for two to either
    Tahiti or St. Moritz, Switzerland.

    Hackers with modems must dial 1-404-827-9584. Then they must type this
    password: 5336241.

    From there, the hacker is on his own to figure out the various access codes
    and commands needed to retrieve the secret message.

    The winner was announced October 24, 1989 at the Federal Computer Show in
    Washington. Taken from USA Today.

- -

10. Groaning Phone Network Survives Millions Of Calls (October 18, 1989) --
     The nation's telecommunications network was flooded Tuesday (October 17)
     night by an estimated 20 million attempted telephone calls from people
     around the nation concerned about friends and family after the earthquake
     in the bay area.

     Except for brief failures, the system did not break down under the record
     load in the areas damaged by the earthquake.

AT&T officials said that as many as 140 million long-distance phone calls were placed Wednesday (October 18), the highest number for a single day in history. Excerpts thanks to John Markoff (New York Times)

>-----------=====END=====---------<