==Phrack Inc.==

Volume Two, Issue 21, File 10 of 11

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN The Legacy...                       ...Lives On PWN
PWN              Phrack World News                  PWN
PWN                 Issue XXI/1                     PWN
PWN                                                 PWN
PWN          Created by Knight Lightning            PWN
PWN                                                 PWN
PWN              Written and Edited by              PWN
PWN         Knight Lightning and Epsilon            PWN
PWN                                                 PWN
PWN The Future...                     ...Is Forever PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

On The Edge Of Forever

November 4, 1988

Greetings and welcome to Phrack World News Issue XXI! As most of you have realized, Taran King and I are back to stay and the tradition of Phrack Inc. lives on. November 17, 1988 marks the Three Year Anniversary of Phrack Inc. and we have never been prouder of our efforts to bring you the best magazine possible.

However, we can not do it alone. Both Taran King and I have been reduced to completely legal status and can not afford the luxury of calling bulletin boards or contacting all the people we would like too.

Epsilon has been helping us a lot by acting as the collection agency for many of the files for Phrack and several news articles as well. Please, if you have a file for Phrack Inc. or an article for PWN contact him or leave mail for The Mentor. And speaking of The Mentor, The Phoenix Project has a new number; (512) 441-3088. Be sure to give it a call.

The article about Pacific Bell in this issue may contain some information that has been seen before. Regardless of that, PWN is a place where such information can be indexed for later reference and helps keep important events and happenings in a certain continuity which is beneficial to everyone.

This issue of Phrack features the Second Special Presentation of Phrack World News, which contains the abridged edition of the WGN Radio Show that dealt with computer hackers and features John Maxfield.

With regard to the file about Teleconnect Long Distance. Hatchet Molly says that now Teleconnect "flags" suspect bulletin boards and if a Teleconnect calling card is used to call one, the card number is cancelled and a new card is mailed to the customer within three days. What a wonderful company policy that is.

For the months ahead, I am working on a file about hackers abroad, mostly focusing on the Chaos Computer Club, which I have begun to have strong relations with, and some other hacker instances in Europe and other parts of the world.

Scheduled for January/February is a file series on the Wide Area Networks; Bitnet and quite possibly ARPAnet, MILInet, NSFnet, IBM's VNET, CCnet, UUCP, CSnet, SPAN, JANet, JUNet, and the list goes on. The main emphasis will be on Bitnet though with secondary emphasis on UUCP and the other networks.

Hope you enjoy this issue and remember... "The Future Is Forever"

:Knight Lightning

Pacific Bell Means Business

October 6, 1988

The following information originally appeared in WORM Newsletter, a publication produced and distributed by Sir Francis Drake. The series of memos presented here are shown to enable the members of today’s hacking community to fully understand the forces at work that seek to bring them down. The memo(s) have been edited for this presentation. -KL

- -

Copy For: Roland Donaldson August 3, 1987
Subject: Unauthorized Remote Computer Access

San Francisco, July 29, 1987
Case Nos.: 86-883, 87-497

T. M. CASSANI, Director-Electronic Operations:

Electronic Operations recently investigated two cases involving a number of sophisticated hackers who were adept at illegally compromising public and private sector computers. Included among the victims of these hackers was Pacific Bell, as well as other local exchange carriers and long distance providers.

Below is a synopsis of the two cases (87-497 and 86-883), each of which demonstrate weaknesses in Pacific Bell’s remote access dial-up systems.

- -

Case No. 87-497

On May 14, 1987, Electronic Operations received a court order directing Pacific Bell to place traps on the telephone numbers assigned to a company known as "Santa Cruz Operations." The court order was issued in order to identify the telephone number being used by an individual who was illegally entering Santa Cruz Operations’ computer and stealing information.

On May 28, 1987, a telephone number was identified five separate times making illegal entry into Santa Cruz Operations’ computer. The originating telephone number was 805-PRE-SUFF, which is listed to Jane Doe, 8731 W. Cresthill Drive, Apt. 404, Thousand Oaks, California.

On June 3, 1987, a search warrant was served at 8731 W. Cresthill Drive, Apt 404, Thousand Oaks, California. The residents of the apartment, who were not at home, were identified as Jane Doe, a programmer for General Telephone, and Kevin Hacker, a known computer hacker. Found inside the apartment were three computers, numerous floppy disks and a number of General Telephone computer manuals.

Kevin Hacker was arrested several years ago for hacking Pacific Bell, UCLA and Hughes Aircraft Company computers. Hacker was a minor at the time of his arrest. Kevin Hacker was recently arrested for compromising the data base of Santa Cruz Operations.

The floppy disks that were seized pursuant to the search warrant revealed Mitnick’s involvment in compromising the Pacific Bell UNIX operation systems and other data bases. The disks documented the following:

o Hacker’s compromise of all Southern California SCC/ESAC computers. On file were the names, log-ins, passwords, and home telephone numbers for Northern and Southern ESAC employees.

o The dial-up numbers and circuit identification documents for SCC computers and Data Kits.

o The commands for testing and seizing trunk testing lines and channels.

o The commands and log-ins for COSMOS wire centers for Northern and Southern California.

o The commands for line monitoring and the seizure of dial tone.

o References to the impersonation of Southern California Security Agents and ESAC employees to obtain information.

o The commands for placing terminating and originating traps.

- The addresses of Pacific Bell locations and the Electronic Door Lock access codes for the following Southern California central offices ELSG12, LSAN06, LSAN12, LSAN15, LSAN23, LSAN56, AVLN11, HLWD01, HWTH01, IGWD01, LOMT11, AND SNPD01.

- Inter-company Electronic Mail detailing new login/password procedures and safeguards.

- The work sheet of an UNIX encryption reader hacker file. If successful, this program could break into any UNIX system at will.

- -

Case No. 86-883

On November 14, 1986, Electronic Operations received a search warrant directing Pacific Bell to trap calls being made to the Stanford University computer. The Stanford Computer was being illegally accessed and was then being used to access other large computer systems throughout the country.

The calls to the Stanford Computer were routed through several different common carriers and through numerous states. Through a combination of traps, traces and sifting through information posted on the Stanford computer, several suspects were identified throughout the United States.

The group of computer hackers who illegally accessed the Stanford computer system were known as "The Legion of Doom." Subsequent investigation indicated that the Legion of Doom was responsible for:

- The use of Stanford University high-speed mainframes to attack and hack ESAC/SCC mini compuuters with an UNIX password hacker file. Password files were then stored on the Stanford systems for other members of the Legion of Doom to use. Login and passwords for every local exchange carrier as well as AT&T SCC/ESAC mini computers were on file.

- The Legion of Doom used the Stanford computers to enter and attack other institutions and private contractors' computers. Some of the contractors' computers were used for national defense research.

On July 21, 1987, eight search warrants were served in three states at homes where members of the Legion of Doom reside. Three of the searches were conducted in California. Steve Dougherty, Senior Investigator-Electronic Operations, accompanied Secret Service agents at the service of a search warrant at 2605 Trousdale Drive, Burlingame, California, which was the residence of Stan QUEST, a sixteen-year-old member of the Legion of Doom. (Correction - Oryan QUEST has never been a member of the Legion Of Doom. -KL)

Dougherty interviewed QUEST, who had used the pseudonym "O'Ryan Quest," (Oryan QUEST) when accessing computers. During the interview, QUEST admitted the following:

- The entering of central offices, (Burlingame, San Mateo, San Bruno, Millbrae) disguised as a Federal Express deliveryman. The entries were done to case out the CO's for the purpose of finding computer terminals with telephones, the locations of switches and bays, the names of Comtechs, and materials related to the operations of the central office. QUEST also claimed to have been in the AT&T Administration office on Folsom Street, San Francisco.

- QUEST's telephone service had been disconnected twice for nonpayment, and twice he had his service restored by impersonating a service representative.

- Learning to test circuits and trunks with his computer by using ROTL and CAROT test procedures.

- Members of the Legion of Doom often accessed test trunks to monitor each other's lines for fun.

o On several occasions QUEST would post the telephone number of a public coin phone for access to his BBS, Digital IDS. He would then access teh Millbrae COSMOS wire center and add call forwarding to the coin phone. He would activate the call forwarding to his home telephone number, securing the identity of his location.

o QUEST would impersonate an employee who had authorization to use a Data Kit and have it turned on for him. When he was done, he would call back and have the Data Kit turned off.

o QUEST also would use his knowledge to disconnect and busyout the telephone services of individuals he did not like. Further, he would add several custom calling features to their lines to create larger bills.

o It was very easy to use the test trunks with his computer to seize another person's dial tone and make calls appear on their bills. QUEST did not admit charging 976 calls to anyone, but he knew of others who did.

o When the Legion of Doom attacked a computer system, they gave themselves five minutes to complete the hacking. If they were not successful in five minutes, they would attempt another system. The Legion of Doom was able to crack a computer in under five minutes approximately 90% of the time.

o QUEST would impersonate employees to get non-published telephone listings. QUEST received the non-published listing for Apple Computer Founder, Steve Wozniak, and members of The Beastie Boys rock group.

o QUEST told Dougherty of one New York member of the Legion of Doom, "Bill from Arnoc," (Bill From RNOC) who has been placing his own traps in New York. Bill from Arnoc (Bill From RNOC) helped QUEST place traps in Pacific Bell.

(Gee Stan, you forgot to admit sneaking over the border. -KL)

The review of the evidence seized at QUEST's residence tends to corroborate all QUEST's statements.

- -

Conclusions

There are some important conclusions that can be drawn from the above two cases regarding future computer system concerns.

o The number of individuals capable of entering Pacific Bell operating systems is growing.

o Computer Hackers are becoming more sophisticated in their attacks.

o Dial-up ports will always be a target for computer entry by a hacker.

o Even dial-up ports with remote callbacks and manually controlled modems can be compromised.

o A hacker can place a central office off-line by overloading a SCC mini computer by improperly placing traps or by putting traps on several DID multi-trunk groups such as MCI or Sprint groups.

o Terrorist or Organized Crime organizations could use this underground computer technology against Pacific Bell or to their own advantage.

o Pacific Bell proprietary data bases such as PTT ESAC or PB2 ESAC could be compromised.

o The integrity of accurate customer billing statements have been compromised through access to the CEBS (Computerized Electronic Billing System) and will remain questionable. A customer can dispute large direct-dialed calls and claim his telephone was accessed by a computer hacker.

- - -

- o Oryan QUEST has a really BIG mouth and would dick over anyone and everyone to overcome his inferiority complex from being an illegal alien without a green card. Outside of the Dan The Operator/Maxfield incident, I have never seen such a mass admission of guilt. To make matters worse, QUEST probably made up most of the incidents to make himself sound like a really big time hacker.

- - -

Recommendations

The information gained as a result of the above investigations should be shared with those individuals responsible for the integrity of our computer systems. Further, an ongoing business partnership between security and the individuals responsible for the integrity of our computer systems should be initiated and maintained to ensure prompt, effective resolution of future computer related security issues.

JOHN E. VENN
Manager-Electronic Operations

Special Thanks To Sir Francis Drake

He's Really Just Out Of Control

PostCon'88

> "I would SHRED everything, because
> we get so much information
> out of the dumpster,
> it's UNREAL..."
>
> -- Control C

Over the last few months there has been a lot of controversy about the mysterious cricumstances regarding Michigan Bell and Control C. To set the record straight, ^C gave me the full details of what happened so I could pass it on to you.

Just prior to leaving Chicago, where ^C had been going to school, he had illegally accessed an AOL system belonging to Michigan Bell. The system operator broke in on him and ^C tried unsuccessfully to pass himself off as a legitimate user. When this did not work, he hung up and did not give it a second thought. Upon returning home to Detroit, he had a message waiting for him to contact the sysop of the AOL system. He calling him and they, accompanied by Michigan Bell security, went out to lunch. To avoid being prosecuted, Control C had to give up all of the information he had on that system and explain how he had gotten in. Since he had cooperated, they let him go without further hassle. Unfortunately, Control C was soon busted again for breaking into his Central Office, but this time he was not going to get off so easily. He had to agree to making a talk show movie and a poster (quoted in the beginning of the article) for Michigan Bell. Both of these items have been distributed across the country to better illustrate the hacker mind-set and as a reminder to destroy important documents that were being thrown away.

While being interrogated by Michigan Bell security department, Control C was shown a list of recently busted hackers from the July 21, 1987 sweep of the country. On this list was Sir Francis Drake, which is how the rumor about SFD being busted last year got started. However, what Control C and Michigan Bell did not know was that when Mark Gerardo was apprehended last year, he was believed to be SFD and as such was entered in their files incorrectly.

Information Provided by Control C

With a little help figuring out the SFD mixup from me and Taran King

:Knight Lightning

North Dakota Nightmare

September 10, 1988

"For Kracking Crue's Docs Avage The Game Is Over"

In March of 1987, the North Dakota members of Kracking Crue (Docs Avage and SpyroGyra (also known as Ractor)) found a local extender and were able to hack out a code. They both lived on campus at North Dakota State University and were able to abuse the code without the worry of being caught because of the campus's Dimension phone system giving them a high degree of anonymity.

They used this code for the entire rest of the school year and nothing had happened to prevent them from abusing it. Because of this lack of security, DA and SG began to believe that the code would be safe for them to use anywhere. The school year ended and the members of the Crue went home. Eventually the Crue discovered a 1-800 number for the long distance service they had been abusing and began to use it once again. However, they were soon to discover that they were not half as safe as they thought.

The LD company had indeed been watching that code, but could not do anything to catch the Crue because of the Dimension system on NDSU campus. Docs Avage started to use the code from his apartment to call SpyroGyra and a few other people and the company got his line tapped and kept a record of where all his calls went to.

In Docs Avage's own words;

> "On July 27th, 1988, I arrived back at my apartment after spending a weekend with my parents at their home. I found it rather interesting to discover three extra cars in the parking lot, one of which was a Dodge Diplomat.
>
> I walked into my apartment and discover two police detectives, two phone officials, and two "computer experts" blissfully dismantling my Apple and all my peripherals. One of my roommates was handcuffed and seated in a chair and my other roommate was kept closely watched as he was sitting in the kitchen. I was asked who I was, and read my rights. I agreed to cooperate. I was busted on a dialup.
>
> The dialup being the one I had hacked out several months before, and gotten quite greedy with it (ok, I overabused the darn thing). In my apartment, I placed around a $1000 worth of calls with it. I had made calls with it before, but not to that extent.
>
> I remained very cooperative, and talked to several phone security representatives, including those from AT&T and U.S. Sprint (I had a printout of 4 Sprint Codes, never had used them, just had them). The phone security people are experts at adverse psychology, and I can successfully say that they did a very good job of scaring me. Nevertheless, I knew that they were trying to play with my brain, so it wasn't as bad as it could have been.
>
> My roommate had been charged with the same offense as myself, Class C Felony Theft of Services (max 5 years/$5000). However, the only thing he contributed to the whole matter was the fact that the telephone account was in his name. The charges were dropped against him.
>
> After almost two months of waiting, the sentence date came. I plead guilty, playing on a deal that my lawyer had made with the state's attorney. The sentence included restitution (which hasn't been determined yet). The phone company is desparately trying to stick me with a large bill, for services that cannot be proven that I had anything to do with; a bill that could stretch up to $5000 (like hell if I'm paying that much), and a very nice little clause called Deferment of Imposition. Basically, I remain on probation until I pay back the restitution, at that time I can go through hearings and prove that I haven't been involved in such activities as for what I was convicted and the charges will not be placed on my record. For the time being however, it's turning out to be monthly payments with supervised probation. Needless to say, I, Docs Avage is retired, at least as as retired as someone in my position can get."

Docs said that he had been looking to retire for some time and that this incident was the final straw. He also added that he was questioned about Jester Sluggo, Phrack Inc., and the Legion of Doom. He did not know anything.

```
                                ==Phrack Inc.==

                      Volume Two, Issue 21, File 11 of 11

             PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
             PWN The Legacy...                       ...Lives On PWN
             PWN                Phrack World News                PWN
             PWN                   Issue XXI/2                   PWN
             PWN                                                 PWN
             PWN           Created by Knight Lightning           PWN
             PWN                                                 PWN
             PWN              Written and Edited by              PWN
             PWN          Knight Lightning and Epsilon           PWN
             PWN                                                 PWN
             PWN The Future...                     ...Is Forever PWN
             PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Man Charged with "Infecting" Computers

May 24, 1988

Fort Worth, Texas (AP) -- A 39-year-old computer programmer is being prosecuted on felony charges of infecting his ex-employer's computers with an electronic "virus," and face up to 10 years in prison if convicted.

Donald Gene Burleson faces a charge of "harmful access to a computer," and is free on a $3,000 bond pending his July 11 trial.

Police described the electronic interference as a "massive deletion" of more than 168,000 records of sales commissions for employees.

Burleson is thought to be the first person charged under the state law prohibiting computer sabotage, which took effect Sept. 1, 1985, about three weeks before the alleged incident, said Davis McCown, chief of the Tarrant County district attorney's economic crimes division.

- -

Jury Selection In First Virus Trial Begins

September 6, 1988

Taken from the Washington Post (September 7, 1988),Page C-1

Fort Worth, Texas (AP) -- Jury selection began today in the criminal trial of a 40-year-old programmer accused of using a computer "virus" to sabotage thousands of records at his former work place. The trial is expected to last about two weeks.

Donald G. Burleson faces up to 10 years in jail and a $5,000 fine if convicted in the trial, a first for the computer industry. Burleson was indicted on charges of burglary and harmful access to a computer in connection with computer damage at a securities firm, said Nell Garrison, clerk of the state criminal district court in Fort Worth. Through his lawyer, Jack Beech, Burleson denies the charges but has declined further comment.

The firm has been awarded $12,000 in a civil lawsuit against Burleson. Pretrial motions were scheduled to be heard today, followed by jury selection, Garrison said.

Burleson is accused of planting a piece of computer software known as a virus in the computer system at USPA&IRA Co. two days after he was fired. A virus is a computer program, often hidden in apparently normal computer software, that instructs the computer to change or destroy information at a given time or after a certain sequence of commands. USPA officials claim Burleson went into the company's offices one night and planted a virus in its computer records that would wipe out sales commissions records every month. The virus was discovered two days later, after it had eliminated 168,000 records.

White Lightning Speaks Up

July 28, 1988

White Lightning was apparently previously accused of being an informant for

Sprint Security with regard to information concerning The Disk Jockey and Compaq.

He left the following message on the Phrack Voice Message System;

> "Yeah, this is White Lightning. I'd like to make an official statement for Phrack Magazine. As far as what happened to The Disk Jockey, Shit, I have no idea, ok? I get on a bridge, I've been out of it for two weeks, I get on Friday night, and fuck, this guy Laser outta 206 is saying I got him busted, I don't know anything about it, ok? As far as Compaq goes, outta 219, Kent, I'd just appreciate it, your information is messed.. <BEEP!> [The Phrack VMS has a beep that lets you know that you only have 10 seconds left.] What the hell is that!? Hello?!? Who is that?!"

Message For White Lightning from Phrack Inc.;

> If you would care to explain your side of the story a little more clearly, we would be happy to listen to what you have to say. We are sure that everyone would be interested. Thank you.

Information Provided By White Lightning

AT&T Links Up With GTE — August 1, 1988

AT&T is stepping up its efforts to boost revenues from telecommunications gear by buying GTE's phone switch business. AT&T will become the leading equipment supplier to GTE's phone companies, which are the main source of the switch operations $500 million in revenues.

AT&T will take a 49% stake in a new company that will comprise GTE's switch manufacturing operations in Illinois and a research and development facility in Phoenix, Arizona. GTE, whose business employs 5,000, is counting on AT&T's technical expertise to support its base of phone switching systems. It also wants out of the phone equipment business. AT&T's main task; making the switches capable of handling the massive voice and computer data transmission requirements anticipated by GTE's phone companies over the next 15 years.

Neither partner disclosed financial terms of the joint venture. But AT&T will own 80% of it by 1993 and 100% by 2003. Its management structure is not yet decided. GTE has made similar moves in recent years that have ended in giving full management control and ownership to its partners. Such deals include one with West Germany's Siemens in communication transmission products and a second with Japan's Fujitsu in office phone systems.

Information Provided by Business Week Magazine

Is There A Doctor In The House? — August 1, 1988

It all started when I met him on a bridge in Texas. No one really understands why he did it or why he chose that particular handle. He seems to have some decent knowledge and would not have had much trouble reaching a high level of notoriety. Unless there is more here than meets the eye.

Doc Holiday/Scott of 713 is an IMPOSTER!

He was doing a pretty good job pretending to be the original Doc Holiday. He had researched all about him, including details concerning his recent bust for COSMOS abuse, and created a framing story to explain how and why he now was Scott instead of Robbie and how his family had moved from Tennessee to Texas. The majority of the phreak/hack community bought the story and he would have gone on unseen except for the return of some folks who had disappeared last fall; Knight Lightning and Taran King. Upon hearing about this Doc Holiday in 713, they already suspected that he was bogus, and once they had spoken to him they knew it was not the original Doc Holiday. To bring a hilarious end to this charade they waited until they could contact the original Doc Holiday to let him in on the exposure.

As destiny would have it, the real Doc Holiday was on vacation and happened to end up spending a weekend in St. Louis, the weekend right after SummerCon '88. So the three of them got together started Scott Holiday talking to further incriminate himself and then let the REAL Doc Holiday introduce himself and have the last laugh.

Scott Holiday was in shock at first and he tried to explain that he had a good reason for doing it, but his mom got on the phone and he had to go.

After this incident, I talked to him voice, and he explained to me that he enjoyed doing this, and it was "the biggest scam" he had ever pulled off, except that you could argue that he did not really pull it off. Seeing as how Scott is quite adept at the art of social engineering, he really had little to no trouble convincing (for lack of a better word) people who did not know the original Doc Holiday. However when he came up against the best, he failed the test miserably.

The point of publicizing this incident is to document that people can be easily fooled and deceit by phone phreaks is not limited to the phone companies. Keep in mind that people are not necessarily whom they claim and in that lies the greatest truth of all.

Information Provided By Epsilon

Special thanks to Knight Lightning and Taran King for the exposure.

Canada Cancels The Underlord — August 3, 1988

"I still Hack!"

The Underlord awoke on February 11, 1988 at 7:30 AM to the sound of his doorbell. Moments later, his mother entered his room to inform him that there were three men waiting to see him. She had a rather puzzled look on her face. He threw on some clothes and ran downstairs to meet his fate head on. The "fat man" showed him a search warrant and informed him that he was under arrest for 7 offenses. They confiscated everything.

The Underlord was escorted to their car (his mother followed behind) and driven off to the police station. They told him something about cameras being all over the station, but it did not matter to him because, "I wasn't going to kill the guy or anything anyway." From there he was taken to a little room, in which he overheard the police playing with my computer, phone, and tapes that they confiscated.

He had to sit there alone for four hours until his dad drove his home and later showed his the papers.

"They said I was being charged for four counts of 'theft of telecommunications' (a real law in Canada), and three counts of mischief."

He was told that the mischief charges were because he called Emergency 911 (although he said he did it through a PBX) and told them obscenities with a friend on three-way.

Practically six months later, on June 16, 1988, The Underlord finally received everything back and went to court. He had to pay $750.00 total and serve eight months probation. However, he only had the three counts of mischief on his record.

He explained that in Canada, if the government wants to make you pay a fine, they must prove that you have enough money to pay it first. However, UL did not and so the authorities said they would drop the charges if he would pay the $750.00.

Information Provided By The Underlord 416
Through The Phoenix Project

Teen Hackers Ring Up Huge Phone Bill — October 7, 1988

By Robert Macy (Associated Press)

Las Vegas, Nevada - Ten teen-age hackers may have run up to $650,000 in telephone calls by tricking phone company computers, and their parents could be liable for the tab, authorities said.

Tom Spurlock, resident agent-in-charge of the Las Vegas Secret Service office, said the teen-agers engaged in Blue Boxing, a technique that enabled them to talk to fellow hackers throughout Europe.

The teen-agers were not taken into custody or charged, but their computers were seized. Spurlock said it will be up to AT&T to decide whether to seek reimbursement once a final tally is obtained.

Virus Hits Unix at Bell Labs   May 13, 1988

Friday the 13th, a devastating virus hit Bell Labs at Murray Hill. Initial reports from survivors indicate that the destruction caused was very widespread, although limited to Sun workstations. Rumor has it that the virus was planted by a disgruntled Sun employee in the Sun Unix kernel. The actual amount of work lost is unknown, as is the Murray Hill policies on frequency of disk backups.

Translation Of 2600 Magazine   Fall 1988

The following appeared on page 46 of 2600 Magazine, Volume 5, Number 3. It was in German and I took the liberty of having a friend who is a member of the Chaos Computer Club in Germany translate it for PWN.

"Hacker" Free Again

One of the heads of the Hamburg CCC, S. Wernery, was released from jail in Paris. The 26-year-old arrived at Hamburg airport yesterday (whenever that was, there was no date on the article). He stated the accusations against him were still being investigated. After having been questioned by a judge he was released from bail, but has to return to Paris at request, though.

:Knight Lightning

Quicknotes

1. BIG! The New Telecom Library Catalog! 1-800-Library. Free, 125 Books, etc.

----

2. The Teleconnect Dictionary; A Glossary of Telecom Acronyms, Terms, and Jargon. Not just definitions...mini essays. $9.95 -- 1-800-LIBRARY.

----

3. Microlog Demo Numbers - Microlog, Irvine, California, makes voice response equipment. Call for demos:

o Micrologl	(800)562-2822
o Immigration and Naturalization	(800)777-7770
o Canadian Embassy	(202)785-1431
o Office of Personal Management	(202)653-8468
o Australian Consulate	(202)797-3161

----

4. Most accurate time in the world; (303)499-7111. It's tied to the atomic clock at the National Bureau of Standards in Boulder, Colorado.

----

5. Sue the United States Postal Service? Good Luck.

   If the US Postal Service loses a package sent by Express Mail, you can't sue for damages the way you can other delivery services.

   Reason: The United States government is immune from lawsuits except when they consent to being sued. The Postal Service has retained this immunity.

----

6. Announcing a new electronic mailbox named Sub-Etha. It is owned and

```
   operated by the Computer Club of Oldenburg, West Germany.

                  Phone number: (0441/777397)  300 Baud N/8/1
```

==Phrack Inc.==

Volume Two, Issue 21, File 1 of 11

Phrack Inc. Newsletter Issue XXI Index

November 4, 1988

Welcome to Phrack Inc. Issue XXI. So far, we've been relatively productive in getting files and getting issues together for the future. If you would like to contribute a file for Phrack Inc., please contact The Mentor or Epsilon and they will forward the files to us, or if you are on any of the connecting networks, send mail and/or files to Taran King's address: C488869@UMCVMB.BITNET. We are pleased to introduce a trilogy pertaining to the security of the phreak/hack community and various aspects thereof. The first file, "Shadows Of A Future Past" and the next two files will be in the next two issues, so be watching for those. It's great to be "back."

Taran King & Knight Lightning

This issue contains the following files;

==Phrack Inc.==

Volume Two, Issue 21, File 2 of 11

== Phrack Pro-Phile XXI ==

The Phrack Pro-Phile's purpose is to present to the reader profiles of older or influential hackers or phreakers that have or do exist. This month's Pro-Phile features a user of past days...Modem Master, a.k.a. Napoleon Solo.

- -

Personal Information
~~~~~~~~~~~~~~~~~~~~

Handle:	Napolean Solo
Call me:	Scott
Past Handle:	Modem Master
Handle Origin:	I used to be a real "Man from UNCLE" fan
D.O.Birth:	March 29, 1970
Current Age:	18 yrs.
Height:	6'0"
Weight:	207 lbs
Eyes:	Hazel
Hair:	Light Brown
Computers:	Apple //+, Apple //gs, normal extra hardware, 2400 baud modem

- -

I started on my way to hackerdom in early 1983 when I bought my first modem, a Networker 300 baud (What a gem!!) to use in my Apple II+. I asked the salesperson for the numbers of the local boards (at the time there were a whole 3 here, and one was an IBM users group board). Well, it just so happened one was an Apple board run on an old version of Networks II, with a sysop who had been known to rip off a local extender here and there. After chatting with him for a while he realized I was one of those eager-to-learn Jr. High kids, so he put me in touch with several other users of his board. Well, one of those was Simon Templar, who would later be the sysop of the Pearly Gates, and I guess to me, about as close a friend a phreak can have that lives 1000 miles a way.

Simon gave me my first code (to an 800 number owned by LDX), and the numbers of some boards where I might pick up some more additional knowledge (IC's Socket, AT&T Phone Center, and Sherwood Forest). Well, after pestering just about anybody that seemed to know ANYTHING, I was on my way. Soon, I was frequenting at least one board in almost every area code. I also learned the advantage of scanning exchanges, I found several local PBXes and a Sprint indial that nobody seemed to known about. That facilitated my "habit" even more and I then found a little Diversi-Dial dubbed "Beandial." That was where I really got off the ground. It was frequented by many knowledgeable phreaks, so between that and all of the BBSes I was on, I had a wealth of knowledge to look to all at my fingertips when I had a question.

Beandial also left me with several good friends, the most notable being Lord Kahz. It also put me in touch with someone rather well known, King Blotto (you should have seen my face the night my phone rang and the guy at the other end said "Hi, this is King Blotto, wanna be on my board?" and gave me the number!). As of the last several years, I have left the mainstream phreaking life, and only look in once in a while through past friends. That may change now, as Taran King and Knight Lightning have shown me that there are in fact TRUE phreaks left. I was beginning to doubt it, hence my absence.

Memorable bulletin boards that I have been on include; The Pearly Gates, AT&T Phone Center, Blottoland (even though I was only actually on during the last phase of its life), and Bean Dial, plus all the normal ones that everybody and his brother were on.

Currently I am enrolled at North Dakota State University, majoring in computer engineering. I work at McDonalds flippin' dem burgers.

Regrets
~~~~~~~

I regret leaving the phreak world in the first place, I was disillusioned with all the little nerds with computers and modems who thought they were phreaks just because some dork they knew gave them a code.

Favorite Things

Chicks: The ones with really big... uh.. Brains! Thats it! Ya know, they stick out their bras.. Uh.. I mean their intelligence protrudes!! Ya! thats it!
People: I like just about anybody who has something interesting and meaningful to talk about (and chicks with big ****)

Music: 70's music like Led Zeppelin, and most heavy metal bands. I also can go for top 40 as long as we aren't talking Whitney, or Jackson, or G. Michael or some other puke like that.

Most Memorable Experiences

The time me and a friend from Idaho called this local guy who THOUGHT he was a phreak. I talked to him on one line, while MIKE talked to him long distance on another, convincing him that AT&T security had really busted his ass. I've never heard ANYONE sound so scared in my life! HAHAH

Starting on my high school's varsity football team for two years instead of the average 0-1 yr.

Some people to mention

Lord Kahz
Cookie Cruncher
Android Base -- for pointing me in the right direction
Simon Templar -- for taking that direction and showing me what to do with it.

All others who have helped me in anyway, whether it be questions I had, or whatever else... Thanks.

Inside Joke

To Kahz: "Hey MM, let's call Mari!"

- -

Serious Section

I think people who abuse CCs are assholes. That does nothing but hurt all of us; all that comes out of it is one person's gain and many people's suffering. Example; Sysops of the board where the inevitably BUSTED asshole posted his CC numbers.

- -

Although he has never met any hackers, Scott feels that there are a few geeks out there based on some of his phone conversations.

Thanks for your time Scott.

Taran King

==Phrack Inc.==

Volume Two, Issue 21, File 3 of 11

```
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
<>                                                                <>
<>                   Shadows Of A Future Past                     <>
<>                   ~~~~~~~~~~~~~~~~~~~~~~~~                     <>
<>            Part One Of The Vicious Circle Trilogy              <>
<>                                                                <>
<>         A New Indepth Look At A Re-Occurring Problem           <>
<>                      by Knight Lightning                       <>
<>                                                                <>
<>                        August 6, 1988                          <>
<>                                                                <>
<><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
```

The Problem?

The fate of the entire modem community for the most part is based on the foundation of computer bulletin boards. These realms of information exchange have become centers of learning and trading various information for thousands of hackers across the United States and even the world.

However, today's security consultants and law enforcement agencies are smarter than ever too and they know where to strike in order to do the most damage. The concept of creating a bulletin board for the purpose of catching hackers was unheard of until The Phoenix Phortress Incident of 1986. The creation of this bulletin board system enabled Sergeant Dan Pasquale of the Fremont Police Department the ability to penetrate the sacred barrier between the phreak/hack community and the rest of the world.

This file will attempt to show the extent of this problem within the community and hopefully will lead readers to discover ways of protecting themselves from the many "venus fly traps" they are likely to encounter. Articles presented in this file are specially edited reprints from past issues of Phrack World News.

The Evidence - The unseen truths reside in the shadows of our past and future.

The following is an excerpt from Phrack World News Issue III;

- -

Phoenix Phortress Stings 7

On March 5, 1986, the following seven phreaks were arrested in what has come to be known as the first computer crime "sting" operation.

Captain Hacker \ Doctor Bob \ Lasertech \ The Adventurer
The Highwayman \ The Punisher \ The Warden

Many of them or other members of Phoenix Phortress belonged to these groups:

High Mountain Hackers \ Kaos Inc. \ Shadow Brotherhood \ The Nihilist Order

Of the seven, three were 15 years old; two were 16; one was 17; and one, 19.

Their charges include:

Several misdemeanors
Trafficking in stolen long distance service codes
Trafficking in stolen credit card numbers
Possession of stolen property
Possession of dangerous weapons (a martial arts weapon)
Charging mail-order merchandise to stolen credit card numbers
Selling stolen property
Charging calls internationally to telephone service numbers

Other phreak boards mentioned include:

Bank Vault (Mainly for credit card numbers and tips on credit card scams)
Phreakers Phortress (Mainly of course for phreak codes and other information)

After serving search warrants early Wednesday morning on the seven Fremont residences where the young men lived with their parents, police confiscated at least $12,000 worth of equipment such as computers, modems, monitors, floppy disks, and manuals, which contained information ranging from how to make a bomb, to the access codes for the Merrill Lynch and Dean Witter Financial Services Firm's corporate computers.

The sysop of Phoenix Phortress was The Revenger, who was supposedly Wally Richards, a 25 year-old Hayward man who "phreaked back east a little" in New Jersey. He took the phone number under the name of Al Davis. However he was really Sgt. Daniel Pasquale of the Fremont Police Department.

When he introduced his board to other computer users, he called it the "newest, coolest, phreak board in town."

Pasquale said he got the idea for the sting operation after a 16-year old arrested last summer for possession of stolen property "rolled them over (narced) He told us all about their operation."

Pasquale used a police department Apple //e computer and equipment, with access codes and information provided by eight corporations, including Wells Fargo Bank, Sprint, and MCI.

Pasquale said he received more than 2,500 calls from about 130 regular users around the country. The police started to make their first case three days after the board went up.

"We had taken the unlisted phone number under the name Al Davis," Pasquale said. "In six days, these kids had the name on the bulletin board. I would have needed a search warrant to get that information."

The arrests were made after five months of investigation by Dan Pasquale.
- -

The Phoenix Phortress incident only led to the arrest of seven hackers. However, at the same time it enabled the law enforcement agencies to gather information about over one hundred other hackers, systems being discussed, anything transmitted in electronic mail on the bulletin board, and most likely gave them information about hundreds of other hackers, bulletin boards, and so forth.

The following is an excerpt from Phrack World News Issue VII;
- -

```
Maxfield Strikes Again                                           August 20, 1986
~~~~~~~~~~~~~~~~~~~~~~
```

Many of you probably remember a system known as "THE BOARD" in the Detroit 313 NPA. The number was 313-592-4143 and the newuser password was "HEL-N555,ELITE,3" (then return). It was kind of unique because it was run off of an HP2000 computer.

On August 20, 1986 the following messages began to appear on THE BOARD;
-   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -   -

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

                          300/1200 baud - 24 hours.

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


Board:   General Information & BBS's
Message: 41
Title:   YOU'VE BEEN HAD!!!
```

To: ALL
From: HIGH TECH
Posted: 8/20/86 @ 12.08 hours

Greetings:

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

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

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

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

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

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

Board: General Information & BBS's
Message: 42
Title: BOARDSCAN
To: ALL
From: THE REAPER

This is John Maxfield of Boardscan. Welcome! Please address all letter bombs to Mike Wendland at WDIV-TV Detroit. This board was his idea.

The Reaper (a.k.a. Cable Pair)

John Maxfield was in general extremely proud of his efforts with THE BOARD and he said that a lot of the people he voice verified should have known it was him. According to John Maxfield, the only reason this sting board was put up was to show "What is currently happening in the phreak/hack community." He said no legal action will be taken at all, and besides, its fattened his "dossiers" on a lot of people!

[The news stories for WDIV-TV 4 appeared in Phrack World News Issue IX.]

- -

Now, this is a classic example of people not learning from other people's mistakes. At some point in time prior to this incident, the number for THE BOARD was posted, it was given a lot of hype and eventually it drew in hackers to THE BOARD like flies to a spider web from which the unsuspecting users never broke free.

That is the point I am trying to make -- today's phreak/hacker must learn to be more security conscious. What makes anyone think that they can trust someone just because they are running a bulletin board? This blind faith is what will be the downfall of many a hacker until they wise up and start paying attention to what they are doing. Safety first; the stakes in this game are a lot higher than no television after school for a week because once a hacker's phone number falls into the wrong hands, the law enforcement community or organizations like the Communications Fraud Control Association (CFCA) can find out everything about you. I know because I have seen their files and their hacker data base is so incredibly large and accurate...its unbelievable.

The following is an excerpt from Phrack World News Issue XIV;

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

Metalland South:  Phreak BBS or MetaliFEDS Inc.?                    June 2, 1987
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Metalland South BBS, at 404-327-2327, was once a fairly well known bulletin board, where many respected members of the hack/phreak community resided. It was originally operated by two guys from Metal Communications, Inc., but it wasn't an MCI club board. The sysop was Iron Man and the co-sysop was Black Lord. Recently, it has come to the writer's attention, that MLS has come under new management, new policies, and possibly a new idea; Sting.

Somewhere around September-October 1986, Iron Man removed all of the hack/ phreak related subboards as well as all G-philes from the system. He was apparently worried about getting busted. The last time this reporter spoke with him, Iron Man said he intended to put the hack/phreak subs back up. Then, not long after this conversation, the number was changed (The original number was 404-576-5166).

A person using the alias of The Caretaker was made co-sysop and Iron Man would not reply to feedback. Everything was handled by The Caretaker [TC from now on]. TC did not allow any hack/phreak subs, but said he would put them up if the users would follow STRICT validation procedures.

Strict validation on MLS includes:

```
^*^  Your Real Name
^*^  Your Address
^*^  Your Voice Phone Number
^*^  A Self-Addressed Envelope (in which he will send back with your account
                                number and password.)
```

It is obvious to see the ramifications here. A board or sysop gets busted and then makes a deal to turn over the board to some company or agency. To make sure that they get who they want, you have to give them all this info, and the only you can get a password is to let them mail it to you, thus guaranteeing that if something illegal is posted under that account, you are responsible, no ifs, ands, or buts.

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

There was more information that went on to prove that Metalland South was indeed some kind of a trap or sting board and the whole aura of mystery surrounding this system made it not worth calling.

Do not EVER give a sysop your address so he can send you your password. There is no need for such information as it can only hurt you severely and would not benefit the sysop in any way that would leave you unharmed.

One other item concerning bulletin boards comes from PWN Issue V where mention of yet another hacker sting board named The Tunnel was discovered in Texas. And lets not forget about TMC's P-80, sysoped by Scan Man, that was responsible for the apprehension of Shawn of Phreakers Quest (also known as Capt. Caveman).

However, do not fool yourself into believing that bulletin boards are the only places you are likely to run into trouble. Regular systems that you like to work with may be just as dangerous if you are not careful. Druidic Death and Celtic Phrost found this out the hard way on the Unix system at MIT as they nearly succumbed to the power of progressive entrapment which would have doomed them both.

The following is an excerpt from Phrack World News Issue XI;

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

MIT Unix:  Victim or Aggressor?                    January 23 - February 2, 1987
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Was the MIT system an innocent victim of hacker oppression or simply another trap to capture unsuspecting hackers in the act?

It all started like this...

[Some posts have been slightly edited to be relevant to the topic]

MIT
Name: Druidic Death
Date: 12:49 am Mon Jan 20, 1986

Lately I've been messing around on MIT's VAX in there Physics Department.

Recently some one else got on there and did some damage to files. However MIT told me that they'll still trust us to call them. The number is:

617-253-XXXX

We have to agree to the following or we will be kicked off, they will create a "hacker" account for us.

<1> Use only GUEST, RODNEY, and GAMES. No other accounts until the hacker one is made. There are no passwords on these accounts.
<2> Make sure we log off properly. Control-D. This is a UNIX system.
<3> Not to call between 9 AM and 5 PM Eastern Standard Time. This is to avoid tying up the system.
<4> Leave mail to GEORGE only with UNIX questions (or C). And leave our handles so he'll know who we are.

Unix
Name: Celtic Phrost
Date: 4:16 pm Mon Jan 20, 1986

Thanks Death for the MIT computer, I've been working on getting into them for weeks. Here's another you can play around with:

617/258-XXXX login:GUEST

Or use a WHO command at the logon to see other accounts, it has been a long time since I played with that system, so I am unsure if the GUEST account still works, but if you use the WHO command you should see the GUEST account needed for applying for your own account.

-Phrost

Unix
Name: Celtic Phrost
Date: 5:35 pm Mon Jan 20, 1986

Ok, sorry, but I just remembered the application account, its: OPEN
Gawd, I am glad I got that off my chest!

-(A relieved)Celtic Phrost.

Also on that MIT computer Death listed, some other default accounts are:

LONG MIKE GREG NEIL DAN

Get the rest yourself, and please people, LEAVE THEM UNPASSWORDED!

MIT
Name: Druidic Death 12
Date: 1:16 am Fri Jan 23, 1987

MIT is pretty cool. If you haven't called yet, try it out. Just PLEASE make sure you follow the little rules they asked us about! If someone doesn't do something right the sysop leaves the gripe mail to me. Check out my directory under the guest account just type "cd Dru". Read the first file.

MIT
Name: Ctrl C
Date: 12:56 pm Sat Jan 24, 1987

MIT Un-Passworded Unix Accounts: 617-253-XXXX

```
ALEX   BILL   GAMES   DAVE   GUEST   DAN   GREG   MIKE   LONG   NEIL  TOM   TED
BRIAN     RODNEY    VRET     GENTILE    ROCKY    SPIKE     KEVIN    KRIS    TIM
```

And PLEASE don't change the Passwords....

         -=>Ctrl C<=-

MIT Again
Name: Druidic Death
Date: 1:00 pm Wed Jan 28, 1987

Ok people, MIT is pissed, someone hasn't been keeping the bargain and they aren't too thrilled about it. There were only three things they asked us to do, and they were reasonable too. All they wanted was for us to not compromise the security much more than we had already, logoff properly, not leave any processes going, and call only during non-business hours, and we would be able to use the GUEST accounts as much as we like.

Someone got real nice and added themselves to the "daemon" group which is superusers only, the name was "celtic". Gee, I wonder who that could have been? I'm not pissed at anyone, but I'd like to keep on using MIT's computers, and they'd love for us to be on, but they're getting paranoid. Whoever is calling besides me, be cool ok? They even gave me a voice phone to chat with their sysops with. How often do you see this happen?

A little perturbed but not pissed...

DRU'

Tsk, Celtic.
Name: Evil Jay
Date: 9:39 am Thu Jan 29, 1987

Well, personally I don't know why anyone would want to be a superuser on the system in question. Once you've been on once, there is really nothing that interesting to look at...but anyway.

-EJ

In trouble again...
Name: Celtic Phrost
Date: 2:35 pm Fri Jan 30, 1987

...I was framed!! I did not add myself to any "daemon" group on any MIT UNIX. I did call once, and I must admit I did hang up without logging off, but this was due to a faulty program that would NOT allow me to break out of it, no matter what I tried. I am sure that I didn't cause any damage by that.

              -Phrost

Major Problems
Name: Druidic Death
Date: 12:20 pm Sat Jan 31, 1987

OK, major stuff going down. Some unidentified individual logged into the Physics Dept's PDP11/34 at 617-253-XXXX and was drastically violating the "agreement" we had reached. I was the one that made the "deal" with them. And they even gave me a voice line to talk to them with.

Well, one day I called the other Physics computer, the office AT and discovered that someone created an account in the superuser DAEMON group called "celtic".

Well, I was contacted by Brian through a chat and he told me to call him. Then he proceeded to nicely inform me that "due to unauthorized abuse of the system, the deal is off".

He was cool about it and said he wished he didn't have to do that. Then I called George, the guy that made the deal and he said that someone who said he was "Celtic Phrost" went on to the system and deleted nearly a year's worth of artificial intelligence data from the nuclear fission research base.

Needless to say I was shocked. I said that he can't believe that it was one of us, that as far as I knew everyone was keeping the deal. Then he (quite pissed off) said that he wanted all of our names so he can report us to the FBI. He called us fags, and all sorts of stuff, he was VERY!! [underline twice] PISSED! I don't blame him. Actually I'm not blaming Celtic Phrost, it very easily could have been a frame up.

But another thing is George thinks that Celtic Phrost and Druidic Death are one and the same, in other words, he thinks that *I* stabbed him in the back. Basically he just doesn't understand the way the hacker community operates.

Well, the deal is off, they plan to prosecute whoever they can catch. Since George is my best friend's brother I have not only lost a friend, but I'm likely to see some legal problems soon. Also, I can forget about doing my graduate work at MIT. Whoever did this damage to them, I hope you're happy. You really messed things up real nice for a lot of people.

Celtic, I don't have any reason to believe you messed with them. I also have no reason to think you didn't. I'm not making an accusation against you, but WHOEVER did this, deserves to be shot as far as I'm concerned. Until this data was lost, they were on the verge of harnessing a laser-lithium produced form of nuclear fission that would have been more efficient than using the standard hydrogen. Well, back to the drawing board now.

I realize that it's hard to believe that they would have data like this on this system. But they were quite stupid in many other areas too. Leaving the superuser account with no password?? Think about it.

It's also possible that they were exaggerating. But regardless, damage seems to have been done.

MIT
Name: Phreakenstein
Date: 1:31 am Sun Feb 01, 1987

Heck! I dunno, but whoever it was, I think, should let himself (the s00per K-rad elyte d00d he is) be known.

I wasn't on MIT, but it was pretty dumb of MIT to even let Hackers on. I wouldn't really worry though, they did let you on, and all you have to prove is that you had no reason to do it.
----Phreak

I wonder...
Name: Ax Murderer 15
Date: 6:43 pm Sun Feb 01, 1987

I highly doubt that is was someone on this system. Since this is an elite board, I think all the users are pretty decent and know right and wrong things to do. Could be that one of the users on this system called another system and gave it out!??

Ax Murderer

It was stupid
Name: Druidic Death 12
Date: 9:21 pm Sun Feb 01, 1987

It seems to me, or, what I gathered, they felt that there were going to be hackers on the system to begin with and that this way they could keep themselves basically safe.

I doubt that it was Celtic Phrost, I don't think he'd be an asshole like that. But I can't say. When I posted, I was pretty pissed about the whole deal. I've calmed down now. Psychic Warlord said something to me voice the other day that made me stop and think. What if this was a set up right from the start? I mean, MIT won't give me specifics on just what supposedly happened, Celtic Phrost denies everything, and the biggest part of it is what George said to me.

"We can forgive you for what you did to us if you'll promise to go straight and never do this again and just tell us who all of your friends are that are on the system".

I didn't pay much attention to that remark at first, now I'm beginning to wonder...

I, of course, didn't narc on anyone. (Who do I know??? hehe)

DRU'

Comments...
Name: Delta-Master
Date: 7:15 am Mon Feb 02, 1987

It wouldn't surprise me if it was some kind of setup, it's been done before.

Delta-Master

[All posts in this article were taken from ShadowSpawn.]

- -

The Solution
~~~~~~~~~~~~

What more is there to say? It definitely looks like there was a setup involved and it probably was not the first time and probably will not be the last time either. So how can you protect yourself?

As far as the bulletin boards go. There is an unwritten rule somewhere that basically says that to be a good sysop, you first have to be a good user. If the sysop of some mystery board is not someone you have seen around for a long time, then I would not call. However, even if it is someone who has been around, references from someone you feel you can trust is a necessity. It all boils down to the reliability of the information and the persons involved.

When dealing with systems like the MIT Unix, remember, if its too good to be true then most likely there will be something that you are not being told. Who in their right mind is going to give free accounts to an important system with delicate information to a group of hackers? Its crazy.

This file will hopefully serve as an informative fresh look at an old game. To me, even if the time I spent putting this article together helps out or saves only one phreak/hacker, I feel my job has been done successfully.

:Knight Lightning

"The Future Is Forever"

The Phoenix Project

=-=
~~~~~~~~~~~~

```
                              ==Phrack Inc.==

                     Volume Two, Issue 21, File 4 of 11

        :.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:
        :.:.:                                                     :.:.:
        :.:                       The Tele-Pages                    :.:
        :.:                       ~~~~~~~~~~~~~~                    :.:
        :.:                   Telenet Nodes/Addresses               :.:
        :.:                                                         :.:
        :.:               Collected by Anonymous Sources            :.:
        :.:                                                         :.:
        :.:    From Europe, United Kingdom, and The Middle East     :.:
        :.:                                                         :.:
        :.:          Imported into the USA by Jester Sluggo         :.:
        :.:                                                         :.:
        :.:                   Special Thanks To Sefi                :.:
        :.:                                                         :.:
        :.:                       October 7, 1988                   :.:
        :.:.:                                                     :.:.:
        :.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:.:
```

This file contains the list of Telenet nodes/addresses you use when you are outside of USA/Canada (Example: United Kingdom, Europe, or the Middle East). Very much 'thanks' goes towards the wonderful, people who worked infinite-months on this. -- Sluggo !!

(* = Passwords that have been removed for this presentation. - KL)

Name	Number	Ext.	User Name	Password	KN	DN	NO	Test	Land
Us Telemail	031102020014		KKCHUNG	********		XX			US
Uni Brighton	023427050015		GUEST	*******		XX			UK
Sysnet Wien	023224221142	MAI	Gast	****		XX			AT
	023424126010604		,5020015	*****/*****		XX			UK
	026243221093001		U 5Jm11964,	*****		XX			
	03422351919169		,10404000	******(*x)		XX			
Z E V	022847911118		EPSON	*****		XX			CH
Altos	45890040004		Woodo	****(*****		XX			DE
Mehlbox HAM	45400090184		Mike	******		XX			DE
E C H O	0270448112		UK85041D	********	XX				NE
Eis - Vax	????????????		????????????	???????????	??	??	??	????	????
B I X	031060057878		Rupert	-----------					US
C.L.I.N.C.H.	4440009031		Gast	****					DE
	45690090125		KO/VMUTIL	******		XX			DE
E X C O N	022849911102001		Call 130	***		XX			CH
	023422351919169		,49000001	*******/****		XX			UK
R M I Aachen	45241090832		Guest (Menue 20.3)	*****					DE
Markt & Tech.	45890010006		EMERY04	???????????	XX				DE
Markt & Tech.	45890010006		EMERY05	???????????		XX			DE
K D D Vax	0440820023		Conf	****		XX			JA
Emery ADO	03106907626		CICS4\D	*****					US
Euronet	023421920100513		Tikatom			XX			NE
Netztest DE	4590049002	ECHO							DE
Netztest AU	05053210001								AU
The Source	0311030100038		Jinatari	*********				DEMO	US
The Source	0311030100038		Josh1	********		XX			US
Delphi	0311061703088		------------	-----------					US
Nuclear Res.	03110500061		Bill	*******		XX			US
E.S.A.	023421920115600		MAR15540			XX			NE
Hazylab	45400030201		User	****		XX			DE
	023421880100300		Mudguest	********		XX		18-8	NE
	4511042301		zzve099/zzueb	******/*******					DE
Datapac	030292100086		-------------	-----------					CA
Dallas	0310600787		-------------	-----------					US
A M P	023422020010700		Use Demo Account						UK
Canada	0302067100901		-------------	-----------					CA
Telenet	0311020200141		Telemailintl	**** ******		XX			US

```
A D P Network |034219200118 |    |1300-7777   |***        |  |XX|  |    | NE |
Hostess       |023421920101013   |Euonet      |*****      |  |XX|  |    | NE |
G D  P T T    |02284410906  |    |mit \G Laeuten NUA *****|  |  |  |    | IT |
Tymnet        |4561040250   |    |            |           |  |  |  |    | DE |
Autonet       |45611040076  |    |            |           |  |  |  |    | DE |
PSS DOC       |02421920101013    |            |           |  |  |  |    |    |
Midnet Gatew. |0234260227227|    |            |           |  |  |  |    | UK |
NUMAC         |0234263259159|    |            |           |  |  |  |    | UK |
Sharp Comp.   |0234219200203|    |,IPSHIP     |           |  |  |  |    | UK |
College LON   |0234219200333|    |,EUCLID     |           |  |  |  |    | UK |
Brit. TELECOM |023421920101030   |,TSTB       |           |  |  |  |    | UK |
Phis. Labtory |0234219709111|    |,NPL1       |           |  |  |  |    | UK |
Phis. Labtory |0234219709210|    |,NPL2       |           |  |  |  |    | UK |
Queen Marry C.|023419806160 |    |,QMC        |           |  |  |  |    | UK |
Atom.Ener.Res.|0234223519111|    |,AERE       |           |  |  |  |    | UK |
Database      |023422351911198   |,DAADA      |           |  |  |  |    | UK |
Uni Leverpool |0234251248248|    |,LIVE       |           |  |  |  |    | UK |
Space Research|0234290524242|    |,RSRERADIO  |           |  |  |  |    | UK |
Brit. Oxig.   |0234293212212|    |,BOC        |           |  |  |  |    | UK |
A M D A H L   |0240515330   |    |,QZIBQZ     |           |  |  |  |    |    |
Cyber         |02405015320  |    |,OZCBQZ     |           |  |  |  |    |    |
H M I         |    45300217 |    |,HMI        |           |  |  |  |    | DE |
S W           |02405020328  |    |,QZXAQZ  via reverse Pad|  |  |  |    |    |
PSS Mail Serv |023421920105 |    |            |           |  |  |  |    | UK |
C E R N       |022846811405 |    |            |           |  |  |  |    |    |
W A X Bank FRA|  45611040187|    |????????????|???????????|  |  |  |    | DE |
Uni Bochum    |  45611040240|    |            |           |  |  |  |    | DE |
Uni Berlin    |  4530040023 |    |            |           |  |  |  |    | DE |
Teleprint SBR |  4568100010 |    |            |           |  |  |  |    | DE |
Max Planc MUC |  45890040220|    |            |           |  |  |  |    | DE |
B B D A       |02062221006  |    |            |           |  |  |  |    |    |
Dialne        |0234212300120|    |            |           |  |  |  |    | UK |
Euclid    LON |0234219200333|    |            |           |  |  |  |    | UK |
Decates       | 44615440371 |    |            |           |  |  |  |    | DE |
R M I Aachen  | 44241040341 |    |            |           |  |  |  |    | DE |
N P L I       |0234219709111|    |            |           |  |  |  |    | UK |
T S T B       |023421920101030   |            |           |  |  |  |    | UK |
U C L         |0234219200300|    |            |           |  |  |  |    | UK |
Dimdi         |45221040006  |    |,DA         |           |  |  |  |    | DE |
Dimdi         |45221040104  |    |,DA         |           |  |  |  |    | DE |
Emery     STR |4471149236   |    |            |           |  |  |  |    | DE |
              |07222211100171    |            |           |  |  |  |    |    |
              |43221093001  |    |U5JM11964,*****        |  |  |  |    | DE |
              |02222632004  |    |ask reply for some NUA’s|  |  |  |    | IT |
              |03106001977  |    |            |           |  |  |  |    | US |
              |023520014300165   |            |           |  |  |  |    | UK |
______________|_____________|____|____________|___________|__|__|__|____|____|

CTR NUA                 NAME,UID,PW,REMARK
=========================================================================
    00000 15000006      FTP FOR ECSVAX
    00000 15000019      FTP FOR EEVAX
    00000 15000034      WEST OF SCOT. COLL. OF AGRIC.
    00000 15000036      FTP FOR CSTVAX
    00000 1500100750    FTP FOR ITS63A
    00000 1500101570    IT SCHOOL 63/40
    00000 16000002      EMAS FRONT END

========================
=   AUS - Australia    =
========================
CTR NUA                 NAME,UID,PW,REMARK
=========================================================================
AUS 05052 28621000      ANGLO/AUSTRALIAN OBSERVATORY
AUS 05052 28621001      CSIRO RADIO-PHYSICS
AUS 05052 28621001      FTP FOR EPPING
AUS 05052 82620000      FTP FOR AUSTEK
AUS 05052 82620000      VAX IN SIDNEY, AUSTRALIA
AUS 05053 210003        MIDAS FOX TEST
```

```
========================
=   CH - Switzerland   =
========================
CTR NUA                 NAME,UID,PW,REMARK
=========================================================================
CH  02284 64110115      DATA.STAR
CH  02284 6811405
CH  02284 681140510,LO  PACX2
CH  02284 6911003       NOS.CYBER,CIA0543,GUEST
CH  02284 79110650      KOMETH.TELEPAC
CH  02284 7911118       ZEV
CH  02284 64110110      DATASTAR
CH  02284 68113150      MANAGEMENT JOINT TRUST

========================
=   D - West Germany   =
========================
CTR NUA                 NAME,UID,PW,REMARK
=========================================================================
D   02624 4890049130
D   02624 5211040026
D   02624 5211040026    PRIMENET
D   02624 5221040002
D   02624 5221040006    MEDICAL DOCS,COLOGNE
D   02624 5221040104    GERMAN MED. INST., COLOGNE
D   02624 5228040187    PI.BONN
D   02624 5300021713
D   02624 5400030029
D   02624 5400030035
D   02624 5400030041
D   02624 5400030046
D   02624 5400030071
D   02624 5400030090    (cierr 1402)
D   02624 5400030104
D   02624 5400030105
D   02624 5400030110    HOST
D   02624 5400030113    (cierr 1402)
D   02624 5400030138
D   02624 5400030150
D   02624 5400030158
D   02624 5400030175
D   02624 5400030187    E2000 HAMBURG VAX
D   02624 5400030201    HASYLAB-VAX
D   02624 5400030202    HERA MAGNET MEASUREMENT VAX 750
D   02624 5400030215
D   02624 5400030259
D   02624 5400030261
D   02624 5400030296    DFH2001I
D   02624 5400030502
D   02624 5400030519
D   02624 5400030566    DFH2001I
D   02624 5400030578    PRIMENET 20.0.4 DREHH
D   02624 5400090184
D   02624 5400091110    DT.MAILBOX
D   02624 5611040009    CENTRE FOR INFO AND DOC,GERMANY
D   02624 5615140282
D   02624 5621040000    TELEBOX
D   02624 5621040000    TELEBOX
D   02624 5621040014    ACF/VTAM
D   02624 5621040025    OEVA
D   02624 5621040026    HOST
D   02624 5621040027    BASF/FER.VAX 8600
D   02624 5621040508    VCON0.BASF.A6
D   02624 5621040516    CN01
D   02624 5621040532
D   02624 5621040580    DYNAPAC MULTI-PAD.25
D   02624 5621040581    DYNAPAC MULTI-PAD.25
D   02624 5621040582
D   02624 5724740001    GERMAN CENTRE FOR TECH.
D   02624 5890040004    ACS.MUNICH
```

```
D   02624 5890040081    NOS.SW.SYS.MUNICH
D   02624 5890040185
D   02624 5890040207    DATABASE OTTOBRUNN
D   02624 5890040207
D   02624 5890040220    HOST
D   02624 5890040221    HOST
D   02624 5890040225    QNTEC.MUNICH
D   02624 5890040262    BDS.UNIX
D   02624 5890040266
D   02624 5890040281    DATUS.PAD
D   02624 5890040510
D   02624 5890040522    PLESSEY.SEMICOND.VAX
D   02624 5890040542
D   02624 589009012
D   02624 5913111       ERLANGEN CYBER 173, NURNBURG

========================
=   F - France         =
========================
CTR NUA                 NAME,UID,PW,REMARK
=========================================================================
F   02080 34020258
F   02080 7802016901
F   02080 38020676      ILL DIVA
F   02080 91040047      SACLAY, FRANCE
F   02080 91190258      LURE SYNCHROTRON SOURCE

========================
=   GB - Great Britian =
========================
CTR NUA                 NAME,UID,PW,REMARK
=========================================================================
GB  02342 12300120      D.I.SERV.
GB  02342 12301186
GB  02342 1300011
GB  02342 1440012
GB  02342 15710104
GB  02342 19200118      AUTONET
GB  02342 19200146
GB  02342 19200154
GB  02342 19200190      PERG.INFOLN.
GB  02342 19200203
GB  02342 19200222
GB  02342 19200300      UNI.LONDON
GB  02342 19200304
GB  02342 19200394      SIANET
GB  02342 19200871
GB  02342 19201002
GB  02342 1920100515    HOSTESS
GB  02342 1920100615
GB  02342 192010100513
GB  02342 1920101013
GB  02342 1920101030
GB  02342 19709111
GB  02342 206411411     UNI.ESSEX
GB  02342 20641141      UNI.ESSEX
GB  02342 22236236
GB  02342 2271511       ---,GUEST,FRIEND (CALL PIP)
GB  02342 2790014302    ALCATEL
GB  02342 12080105
GB  02342 12300120      DIALOG VIA DIALNET IN LONDON
GB  02342 123002920
GB  02342 12301281      ONE TO ONE COMMS
GB  02342 13900101      ALVEY MAIL FACILITY
GB  02342 1390010150    ALVEY MAIL SYS FTP
GB  02342 19200100      UNI OF LONDON COMPUTING CENTRE
GB  02342 19200171
GB  02342 19200220      BRITISH LIBRARY ON-LINE SYSTEM
GB  02342 19200300      UNIVERSITY COLLEGE, LONDON
GB  02342 19200394      COMPUTER SERVICES, LONDON
GB  02342 1920100513    BRITISH TELECOM SERVICES
GB  02342 1920100620    P. ON-LINE BILLING SERVICE
GB  02342 1920102517
GB  02342 20641141      UNI OF ESSEX FTP
GB  02342 2223616300    CARDIFF UNIVERSITY MULTICS
GB  02342 27200110      GEAC 8000 ITI
GB  02342 27200112      HEWLETT PACKARD LABS, BRISTOL
GB  02342 31300101      PRIME OFFICE, EDINBURGH
GB  02342 31300102      FORESTRY COMMISSION FTP
GB  02342 31300105      LATTICE LOGIC LTD
GB  02342 31300107
GB  02342 34417117      ICL BRACKNELL
GB  02342 41200107
GB  02342 4620010243    ICL WEST GORTON 'B' SERVICE
GB  02342 4620010248    ICL WEST GORTON 'X' SERVICE
GB  02342 4620010277    FTP FOR ICL WEST GORTON PERQ
GB  02342 4620010277    ICL WEST GORTON PERQ
GB  02342 46240240      ICL KIDSGROVE
GB  02342 53300124      LEICESTER
GB  02342 5820010604    AGRENET CPSE
GB  02342 60227227      UNI OF LEICESTER FTP
GB  02342 61600133      IBM - SALE
GB  02342 61600133      IBM SALE FTP
GB  02342 61643365      ICLBRA
GB  02342 6164336543    ICL WEST GORTON 'B' SERVICE
GB  02342 6164336548    ICL WEST GORTON 'X' SERVICE
GB  02342 6164336577    FTP FOR ICL WEST GORTON PERQ
GB  02342 6164336577    ICL WEST GORTON PERQ
GB  02342 64200136      PRIMENET
GB  02342 70712217      HATFIELD POLYTECHNIC
GB  02342 75312212      BRITISH OXYGEN
GB  02342 75312212      THE WORLD REPORTER
GB  02342 78228282      ICL LETCHWORTH
GB  02342 78228288      ICL LETCHWORTH
GB  02342 90468168
GB  02342 90840111      SCICON, SOUTH ENGLAND
GB  02342 93765265      BRITISH LIBRARY LENDING DIVI.

========================
=   I - Italy          =
========================
CTR NUA                 NAME,UID,PW,REMARK
=========================================================================
I   02222 620021        EUROPEAN SPACE AGENCY, ROME

========================
=   IRL - Ireland      =
========================
CTR NUA                 NAME,UID,PW,REMARK
=========================================================================
IRL 02724 31540002      EUROKOM (UNIV COLLEGE DUBLIN)
IRL 02724 3154000803
IRL 02724 3154000803    IRL.HEA.TCD.DEC20 (TOPS-20)
IRL 02724 3159000630

========================
=   N - Norway         =
========================
CTR NUA                 NAME,UID,PW,REMARK
=========================================================================
N   02422 11000001      DEC-10, OSLO UNI

========================
=   NL - Netherlands   =
========================
CTR NUA                 NAME,UID,PW,REMARK
=========================================================================
NL  02041 294002        DUPHAR WEESP,HOLLAND

========================
=   S - Sweden         =
========================
CTR NUA                 NAME,UID,PW,REMARK
=========================================================================
S   02402 00310228      UNI.LUND
S   02405 015503        GOTTENBURG, SWEDEN
S   02405 02032832      ODEN, SWEDEN

========================
=   SF - Finland       =
========================
CTR NUA                 NAME,UID,PW,REMARK
=========================================================================
SF  02442 02007         CANDE IN FINLAND
SF  02442 03008         VAX 11/750 IN FINLAND
========================
=   USA = USA          =
========================
CTR NUA                 NAME,UID,PW,REMARK
=========================================================================
USA 03020 58700900      DATAPAC
USA 03020 60100010      UNI.ALBERTA
USA 03106 0050
USA 03106,DELPHI        TYMNET
USA 03110 2020014275
USA 03110 20423
USA 03110 4150002000    D.I.SERV.
USA 03110 60300020      COL.DARTMOUTH
USA 03106               GATEWAYS
USA 03106 000000        Unknown
USA 03106 000023
USA 03106 000032
USA 03106 000034
USA 03106 000050        NLM MIS bsd unix
USA 03106 000060
USA 03106 000065
USA 03106 000066        BCS ** to be investigated **
USA 03106 000071
USA 03106 000081        COMPUTONE ** to be investigated **
USA 03106 000093
USA 03106 000096        REMOTE COMPUTING
USA 03106 000098        LOCKHEED DATAPLAN
USA 03106 000101        SIO
USA 03106 000113        1=LINK SYS
                        3=BANK OF USA,ABACIS,DIRECTOR)
USA 03106 000155
USA 03106 000173        TYMNET/CODAN NET. Inter-link
USA 03106 000179        LBL
USA 03106 000188
USA 03106 000210
USA 03106 000227
USA 03106 000241        HOST    A,4 BAIFS  BANK OF AMERICA
                                S,3 SFDCS1
USA 03106 000249
USA 03106 000280        HONEYWELL MPL
USA 03106 000289        ROSS SYSTEM (32,26,2,3,12,20,21)
                        7,5,17,18,47,51,A - unknown VAX systems
                                    14,15 - RSTS ROSS SYSTEMS
                            9,43,44,45,48 - MICRO VMS VAX
USA 03106 000307        INFOMEDIA SERVICE CENTRE ONE
USA 03106 000315
USA 03106 000327
USA 03106 000331        (VM/370 system)
USA 03106 000377        MONSANTO AD RESEARCH PRODUCTION
                        APPLICATION NETWORK
USA 03106 000379
USA 03106 000401        TMCS PUBLIC NETWORK
USA 03106 000411        TYMNET/BOSTON/TNS-PK1 interlink
USA 03106 000423        CORPORATE COMPUTER SERVICES
USA 03106 000424        (link to 4 VM/370 systems)
USA 03106 000428        AAMNET
USA 03106 000439        MIS 2 (cierr 1402)
USA 03106 000463        SIGNETICS VM/370
USA 03106 000464
USA 03106 000496
USA 03106 000497        UBS COMPUTER SYSTEMS (host)
USA 03106 000498
USA 03106 000515        ONTYME II
USA 03106 000581
USA 03106 000585        C/C/M
USA 03106 000619        SPNB VM/370
USA 03106 000632        TYMNET/TRWNET inter-link
USA 03106 000633        PUBLIC TYMNET/TRWNET INTERLINK
USA 03106 000636        LINK TO TRAC SYSTEMS (over one 120 terminal)
USA 03106 000646
USA 03106 000664
USA 03106 000674
USA 03106 000685        MTS-A RESEARCH (HOST) 10 - TOPS-20,
                                              12 - UNKNOWN
                                              14 - UNKNOWN,
                                              20 - MTS(C) TOPS-20
                                              30 - MTS(F) TOPS-20,
                                              32 - UNKNOWN
USA 03106 000704        TYMNET-CUP(704)/DUBB-NTS(4) inter-link
USA 03106 000715        TYMNET TEST system
USA 03106 000729        (VM/370 system)
USA 03106 000731
USA 03106 000742        LADC L66A
USA 03106 000755        CORPORATE COMPUTER SERVICES
USA 03106 000759
USA 03106 000760        DEC host Solar Cae/Cam
USA 03106 000761        DOJ host
USA 03106 000788        TYMNET-6754/McGRAWHILL inter-link
USA 03106 000793        J&J HOST
USA 03106 000798
USA 03106 000800        link to: CSG VAX, CYBER 815, SB1,
                                 SB2, SB3, SCN-NET
USA 03106 000821
USA 03106 000832        ONTYME II
USA 03106 000842
USA 03106 000850        CISL SERVICE MACHINE
USA 03106 000859
USA 03106 000871
USA 03106 000898        P&W
USA 03106 000932
USA 03106 001010        DITYMNET01
USA 03106 001024
USA 03106 001030
USA 03106 001036        IBM1
USA 03106 001042        IDC/370
USA 03106 001043
USA 03106 001053        STRATEGIC INFORMATION
USA 03106 001056        SYNTEX TIMESHARING
USA 03106 001105        HOST SGNY  1 - VAX II PRODUCTIONS SYSTEM
                                   3 - VAX II PRODUCTIONS SYSTEM
                                   (tried to 5)
USA 03106 001110
USA 03106 001134        COMPUSERVE
USA 03106 001141        MESSAGE SERVICE SYSTEM (FOX)
USA 03106 001143
USA 03106 001152
USA 03106 001158        TYMNET USER SERVICE
USA 03106 001227        ACF2
USA 03106 001288
USA 03106 001304        ONTYME II
USA 03106 001309
USA 03106 001316
USA 03106 001320
USA 03106 001328
USA 03106 001330        MULTICS, HVN 862-3642
USA 03106 001341
USA 03106 001358
USA 03106 001361        THOMPSON COMPONENTS-MOSTEK CORPORATION
USA 03106 001383        HOST 1,A - TILLINGHAST BENEFITS T.SHAR.SYS.
                             2,C - TILLINGHAST INSURANCE T.SHAR.SYS.
                             4,D - OUTDIALS
                             6   - TILLINGHAST VAX 8600
                             (tried to 10,G)
USA 03106 001391        SOCAL
USA 03106 001399        C80
USA 03106 001400        TMCS PUBLIC NETWORK
USA 03106 001410        DATALYNX/3274 TERMINAL
USA 03106 001417
USA 03106 001434        (host system) - double digits
                        VM is active, tried  to BZ
USA 03106 001438
USA 03106 001443
USA 03106 001467        STN INTERNATIONAL
USA 03106 001482        FNOC DDS
USA 03106 001483        ADR HEADQUARTERS
USA 03106 001487
USA 03106 001488        (cierr 1402)
USA 03106 001502        ARGON NATIONAL LAB
USA 03106 001508        IDC/370
USA 03106 001509
USA 03106 001514        (HOST) DC-10
USA 03106 001519
USA 03106 001533        SBS DATA CENTRE
USA 03106 001557
USA 03106 001560
USA 03106 001572        PRIMECON NETWORK (system 50)
USA 03106 001578
USA 03106 001589
USA 03106 001594        CON138
USA 03106 001611
USA 03106 001612        TYMNET-NEWARK/TSN-MRI inter-link
USA 03106 001616        TYMNET-5027/McGRAW HILL inter-link
USA 03106 001624
USA 03106 001642        Host, A - CORNELLA (system choices displayed)
USA 03106 001659        BYTE INFORMATIO EXCHANGE,GUEST,GUEST
USA 03106 001663        PEOPLE LINK
USA 03106 001665
USA 03106 001709
USA 03106 001715        TYMNET/BOFANET inter-link
USA 03106 001727
USA 03106 001757
USA 03106 001763
USA 03106 001765
USA 03106 001766        PRIMENET
USA 03106 001769        S.C. JOHNSON & SON R & D COMPUTER SYSTEMS
USA 03106 001789        HOST WYLBUR.N - CICS TWX A,C,D,G,H,P,R,S,V,Z
USA 03106 001799        (HOST) classes: 5 - VM/370, 20,23,26 UNKNOWN
                        (TRIED TO 32)
USA 03106 001807
USA 03106 001817        MITEL Host (no luck up to sys 20)
USA 03106 001819        TMCS PUBLIC NETWORK
USA 03106 001831        MULTICS
USA 03106 001842
USA 03106 001844
USA 03106 001851
USA 03106 001853
USA 03106 001854
USA 03106 001857
USA 03106 001864        SUNGARDS CENTRAL COMPUTER FACILITY NETWORKS
USA 03106 001873        MULTICS MR10.2I
USA 03106 001874
USA 03106 001880
USA 03106 001881
USA 03106 001892        PRIMENET (certain hours)
USA 03106 001897
USA 03106 001912
USA 03106 001977
USA 03106 002040
USA 03106 002041
USA 03106 002046        MITEL CORP IN KANATA
USA 03106 002050        TYMNET/BOFANET inter-link,ABACIS,SFDCS1
                                       1 - link,
                                       2 - SFDCS1,DIRECTOR,
                                       3 - ABACIS,ABACIS
                                       A - ABACIS 2
                        (note, Abacis may be used as
                         U/N for many systems on tymnet)
USA 03106 002060
USA 03106 002070
USA 03106 002086
USA 03106 002095        COMODEX ONLINE SYSTEM
USA 03106 002098        D & B,COMMANDO,DIRECTOR,FUCK
USA 03106 002099        D & B,COMMANDO,ASSASIN,SHIT
USA 03106 002100        D & B,COMMANDO,DIRECTOR,FUCK,RAIDER
USA 03106 002109        TYMNET/15B  (inter-link)
USA 03106 002164        MITRE SYSTEM
USA 03106 002179
USA 03106 002188
USA 03106 002196
USA 03106 002200
USA 03106 002201
USA 03106 002212
USA 03106 002222
USA 03106 002286        Primenet TFGI
USA 03106 002299        CONSILIUM
USA 03106 002306
USA 03106 002314
USA 03106 002320
USA 03106 002329        MFE
USA 03106 002330
USA 03106 002384
USA 03106 002387        ** TO BE INVESTIGATED **
USA 03106 002391
USA 03106 002408
USA 03106 002418        UNC VAX
USA 03106 002443        DATAHUB
USA 03106 002445
USA 03106 002446
USA 03106 002453        PRIMENET
USA 03106 002470
USA 03106 002496        NOS SOFTWARE SYSTEM
USA 03106 002519
USA 03106 002537
USA 03106 002539        TYMNET/CIDN Inter-link
USA 03106 002545        CENTRE FOR SEISMIC STUDIES
USA 03106 002578        SEL
USA 03106 002580        ** to be investigated **
USA 03106 002584        (HOST)
USA 03106 002602        MULTICS
USA 03106 002603        MULTICS system M
USA 03106 002609        CON5
USA 03106 002614        HOST
USA 03106 002623        VAX/VMS,GUEST
USA 03106 002624        SUNEX-2060 TOPS-20
USA 03106 002632
USA 03106 002635        QUOTDIAL
USA 03106 002646
USA 03106 002657
USA 03106 002667
USA 03106 002677        THE TIMES
USA 03106 002694        PVM3101,SPDS/MTAM, MLCM,VM/SP,STRATUS-1,STRATUS-2
USA 03106 002700        ANALYTICS SYSTNE
USA 03106 002709        AUTONET
USA 03106 002713
USA 03106 002730
USA 03106 002732
USA 03106 002744
USA 03106 002765        MULTICS
USA 03106 002768        (cierr 1402)
USA 03106 002779        SCJ TIMESHARING
USA 03106 002790        VM/370
USA 03106 002800
USA 03106 002807        ISC
USA 03106 002824
USA 03106 002842
USA 03106 002843
USA 03106 002851        CHEM NETWORK DTSS
USA 03106 002864        RCA SEMICUSTOM
USA 03106 002871        (same as 5603)
USA 03106 002875        (cierr 1402) MTECH/COMMERCIAL SERVICES DIVISION
USA 03106 002889        ** to be investigated **
USA 03106 002901
USA 03106 002910        (CIERR 1402)
USA 03106 002921        CHRYSLER NETWORK
USA 03106 002971
USA 03106 002991        US MIS IS400
USA 03106 002995        VAIL VAX
USA 03106 002998        TYMNET/FIRN DATE NETWORK Inter-link
USA 03106 003002        MULTICS
USA 03106 003009
USA 03106 003028        DCOM class - 0
USA 03106 003030        DCOM class - 0 *investigate*
USA 03106 003036
USA 03106 003050        ATPCO FARE INFORMATION SYSTEM
USA 03106 003062        (Host) class 0,1 ** to be investigated **
USA 03106 003079        VM/370
USA 03106 003092        TYMNET/PROTECTED ACCESS SERVICE SYS. Inter-link
USA 03106 003168        VM/370
USA 03106 003214        VM/370
USA 03106 003220        VM/370
USA 03106 003221        VM/370
USA 03106 003248
USA 03106 003284        COMPUFLIGHT
USA 03106 003286        VAX
USA 03106 003295        TYMNET/PROTECTED ACCESS SERVICE SYSTEMS
                        Inter-link,ABACIS
USA 03106 003297        TYMNET/PROTECTED ACCESS SERVICE SYSTENS
                        Inter-link,ABACIS
USA 03106 003310
USA 03106 003321
USA 03106 003356
USA 03106 003365
USA 03106 003373        IOCSQ
USA 03106 003394        (HOST WYN) 1 - VM/370,
                                   2 - VM/370,
                                   3 - IKJ53020A,
                                   5 - VM/370
                                   6 - NARDAC  <CR> - NARDAC
USA 03106 003420
USA 03106 003443        ** TO BE INVESTIGATED **
USA 03106 003520
USA 03106 003527
USA 03106 003529        (CIERR 1402)
USA 03106 003534
USA 03106 003564        (CIERR 1402)
USA 03106 003568        OAK TREE SYSTEMS LTD
USA 03106 003572        NORTH AMERICA DATA CENTRE
USA 03106 003579
USA 03106 003604        VM/370
USA 03106 003605
USA 03106 003623
USA 03106 003797
USA 03106 003828        TYMNET/AKNET Inter-link
USA 03106 003831
USA 03106 003846        (same as 5603)
USA 03106 003879        (CIERR 1402)
USA 03106 003882        BEKINS COMPANY MUS/XA ACF/VTAM NETWORK
USA 03106 003946
USA 03106 003973        FORD -ELECTRICAL ELECTRONIC DIRECTORY
USA 03106 003994        FORD -ELECTRICAL ELECTRONIC DIRECTORY
USA 03106 004007
USA 03106 004016
USA 03106 004028        MDS-870
USA 03106 004041        RCA GLOBCOM'S PACKET SWITCHING SERICE
USA 03106 004092
USA 03106 004125
USA 03106 004129        ---,ABACIS
USA 03106 004131        ---,ABACIS
USA 03106 004137        TSO, VM/370
USA 03106 004173
USA 03106 004174        VM/370
USA 03106 004202
USA 03106 004206        MAINSTREAMS
USA 03106 004210
USA 03106 004288
USA 03106 004296
USA 03106 004341        (HOST) 2 - VM/370, T - VM/370, 1,3,4,A,C,E,Z
USA 03106 004350        AEC ** TO BE INVESTIGATED **
USA 03106 004365        NATIONAL LIB.OF MEDICINE'S TOXIC.DATA NETWORK
USA 03106 004389        BUG BUSTING MACHINE OF NYN
USA 03106 004468        BETINS COQ,6R5u(VACF/VTAM NETWORK
USA 03106 004472        ROLM CBX DATA-SWITCHING
USA 03106 004499        MRCA
USA 03106 004514        US MISS (IS400)
USA 03106 004530        (Host) active centre AA, ** investigate ! **
USA 03106 004541        (Host)
USA 03106 004545        HMN
USA 03106 004555        2 CASTER BACKUP
USA 03106 004562
USA 03106 004573
USA 03106 004579
USA 03106 004580        TSO
USA 03106 004619
USA 03106 004645
USA 03106 004702        PRIMENET
USA 03106 004706        (Host)
USA 03106 004726        NALCOCS DEC-10
USA 03106 004743        TYMNET INFO SERVICE
USA 03106 004755        STORE DEVELOPMENT MACHINE
USA 03106 004759        (Host)
USA 03106 004791        MIS GROUP/CAD DIVISION/COMPUTERLAND CORP.
USA 03106 004828        VTAM007
USA 03106 004865        GAB BUSINESS SERVICES
USA 03106 004869
USA 03106 004898
USA 03106 004946
USA 03106 004949
USA 03106 004956        (Host)  0 - Vax,
                                1 - KL1,
                                2 - KL,
                                3 - IBM,
                                8 - VAX 2,
                               11 - PC1-130
USA 03106 004957        NEC SEMI-CUSTOM DESIGN CENTRE
USA 03106 005018        (Host)
USA 03106 005034        (cierr 1402)
USA 03106 005058
USA 03106 005062        UIS SUPPB=MQDIRNET
USA 03106 005080
USA 03106 005082        COMPAQ
USA 03106 005107
USA 03106 005119        (Host)
USA 03106 005124        OPERATIONAL INFO SYSTEM VAX
USA 03106 005136        ** to be investogated **
USA 03106 005224        (Host)
USA 03106 005229        UNIV.OF PENNSYLVANIA SCHOOL OF ARTS AND SCIENCE
USA 03106 005267        CHANEL 01
USA 03106 005320        (Host) US DIGMAL COMPUTER SERVICES
USA 03106 005433
USA 03106 005438
USA 03106 005453
USA 03106 005463        VM/370
USA 03106 005528        STRATUS/32
USA 03106 005531        STRATUS/32
USA 03106 005539        VA II/730
USA 03106 005564        STRATUS/32
USA 03106 005566        Host sys  A,1 - 3M TRAC SERVICE system ALICE
                                  B,2 - 3M TRAC SERVICE system BAMBI
                                    3 - 3M TRAC SERVICE system CHIP
                                    4 - 3M TRAC SERVICE system DALE
                                    5 - 3M TRAC SERVICE system ELLIOT
                                    6 - 3M TRAC SERVICE system FLOWER
                                 12,7 - 3M TRAC SERVICE system GRUMPY
                                    8 - TRAC CLUSTER VIRGO, SYSTEM HAPPY
                                    9 - TRAC CLUSTER VIRGO, SYSTEM ISABEL
                                   10 - TRAC CLUSTER VIRGO, SYSTEM JUMBO
                                   11 - TRAC CLUSTER VIRGO, SYSTEM KANGA
                                   13 - VAX
                                   18 - DIGITAL ETHERNET
                                   28 - unknown
                                   31 - CIERR 1402
                                   32 - CIERR 1402
                                   33 - CIERR 1402
                                   34 - CIERR 1402
                                   35 - CIERR 1402
                                   36 - unknown
                                   37 - CIERR 1402
                                   38 - unknown
                                   40 - CPU-STP-A
                                   41 - CIERR 1402
                                   43 - UNKNOWN
                                   44 - ATLAS VAX
                                   45 - FAXON INFO SERVICE
                                   46 - ELECTRICAL PRODUCTS
                                        LABORATORY VASX II/750
                             47,48,49 - unknown
                                   52 - SERC COMPUTER RESOURCES VAX
                                   53 - unknown
                                   54 - SERC COMPUTER RESOURCES VAX
                                   55 - BDS UNIX
                                81,61 - TRAC CLUSTER LIBRA system LADY
                                   62 - TRAC CLUSTER LIBRA system MICKEY
                                   63 - TRAC CLUSTER GEMINI system NEMO
                                   64 - TRAC CLUSTER GEMINI system OWL
                                   65 - TRAC CLUSTER LIBRA system PLUTO
                                   67 - TRAC CLUSTER GEMINI system QUASAR
                                   68 - unknown
                                   70 - TRAC TIMESHARING VAX
                                   71 - TRAC TIMESHARING VAX
                                   72 - TRACE TIMESHARING VAX
                                   73 - DIGITAL ETHERNET TERMINAL SERVER
                                   74 - TRAC TIMESHARING VAX
                                   76 - TRAC TIMESHARING VAX
                                   81 - TRAC TIMESHARING VAX
USA 03106 005569        STRATUS/32
USA 03106 005571        STRATUS/32
USA 03106 005603        (Host) systems 1,2,3,4,5,C (5=Outdial)
USA 03106 005622
USA 03106 005683        TECHNICAL SUPPORT PRODUCTIONS
USA 03106 005697
USA 03106 005702        AUTH
USA 03106 005704        SPOOL
USA 03106 005705
USA 03106 005706
USA 03106 005707
USA 03106 005708        IFPSE
USA 03106 005709        IFPSE
USA 03106 005711        IFXMP
USA 03106 005712
USA 03106 005725        PRIMENET
USA 03106 005744        (Cierr 1402)
USA 03106 005755        Host system, active links = A,B,C,E,F,H,G,I,
                                                    J,K,L,M,O,P,Q,R,
                                                    S,T,U,V,W,X,Y,Z
USA 03106 005758        SEI/MUS SYSTEM
USA 03106 005805
USA 03106 005818        CORPORATE MANAGEMENT INFO SYSTEMS
USA 03106 005846        (Host)
USA 03106 005897
USA 03106 005903
USA 03106 005941
USA 03106 005969        PLESSEY SEMICONDUCTORS-IRVINE
USA 03106 005984        CREDIT AGRICOLE-USA
USA 03106 006019        PRIMENET
USA 03106 006046
USA 03106 006093        NALCO CHEMICAL COMPANY NETWORK
USA 03106 006121        CORPORATE MANAGEMENT INFO SERVICE
USA 03106 006187
USA 03106 006190        CLEVELAND
USA 03106 006191
USA 03106 006227
USA 03106 006251
USA 03106 006281        EDCS
USA 03106 006283        EDCS
USA 03106 006296
USA 03106 006432        EASYLINK
USA 03106 006434        EASYLINK
USA 03106 006440
USA 03106 006590        US CENTRA SERVICE
USA 03106 006597
USA 03106 006686
USA 03106 006722        INTERNATIONAL NETWORK
USA 03106 006828
USA 03106 006832        A&A DATANET (SYSTEMS 1,8,0,14)
USA 03106 006833        (GO AWAY)
USA 03106 006834
USA 03106 006835        TOC
USA 03106 006867        DATABILITY TIMESHARING SYSTEM II
USA 03106 006994
USA 03106 007028
USA 03106 007103
USA 03106 007177
USA 03106 007272        (CIERR 1402)
USA 03106 007351        PRIMENET
USA 03106 007352        PRIMENET
USA 03106 007377
USA 03106 007596        (Host)  A - VM/370, B - VM/370
USA 03106 007640

- J. Sluggo
```

```
                                ==Phrack Inc.==

                      Volume Two, Issue 21, File 5 of 11

           /\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\
           \/                                                    \/
           /\              Satellite Communications              /\
           \/              ~~~~~~~~~~~~~~~~~~~~~~~~              \/
           /\                  By Scott Holiday                  /\
           \/                    July 11, 1988                   \/
           /\                                                    /\
           \/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/\/
```

Satellite communications systems employ microwave terminals on satellites and ground to earth stations for highly reliable and high-capacity communications circuits. The communication satellites are positioned in geosynchronous orbits about 22,000 miles above the earth. Thus the rotation of the satellite matches that of the earth, and the satellite appears motionless above earth stations. Three equally spaces satellites are required to cover the entire world.

The satellite's microwave terminals receive signals from an earth station and retransmit those signals on another frequency to another earth station. Because of the long distances involved, the round-trip communications path takes about a half second. This is referred to as the propagation delay. The propagation delay on a regular terrestrial phone line is about 1 millisecond (ms) per 100 miles.

Each microwave terminal on the satellite, designated as a repeater or transponder, includes a receiver for uplink transmissions and a transmitter for down-link transmissions. Separate bands of frequencies for up-link and down-link transmissions are designated in the 1.5-30 GHz frequency range (1.5 GHz is equal to 1,500,000,000 Hz, or 1.5 billion hertz). Typical frequencies for communications satellites are 4-6 GHz for INTELSAT 5 and 12-14 GHz for Anik-B, a Canadian satellite.

Each satellite transponder typically has twelve 36-MHz channels which can be used for voice, data, or television signals. Early communications satellites had some 12 to 20 transponders, and the later satellites have up to 27 or more transponders. INTELSAT 5, for example, has a total of 27 or more transponders providing 24,500 data/voice channels, one transponder providing two 17.5-MHz TV channels, and one SPADE transponder with 800 channels. SPADE (Single carrier per channel, Pulse code modulation, multiple Access, Demand assignment) is a digital telephone service which reserves a pool of channels in the satellite for use on a demand-assignment basis. SPADE circuits can be activated on a demand basis between different countries and used for long or short periods of time as needed.

Propagation Delay:

The approximate quarter second one-way propagation delay in satellite communications affects both voice telephone and data communications. Users of voice communications via satellite links face two objectionable characteristics; delayed speech and return echoes. Echo suppressors are installed to reduce the return echoes to an acceptable level. Data communications operations face more serious problems caused by propagation delay. Line protocol and error detection/correction schemes are slowed down dramatically by the quarter second of delay. User response time requirements can be difficult to meet because of these cumulative effects.

Satellite delay compensation units are available to ensure a connection and afford better operation for the terrestrial communications terminal that were never designed to deal with the propagation delay of communications satellites. One delay compensation unit is required at each final destination. The units reformat the data into larger effective transmission blocks so that retransmision requests are sent back less frequently. This reduces the number of line turnarounds, each of which requires about a quarter second to go from or return to the destination terminal or computer. One error detection and correction method used, called GO-BACK-N, requires that all blocks of data held in the transmitting buffer, back to the one with the error in it, must be retransmitted. A more efficient method is to retransmit only the block of data with the error, but this requires more logic in the equipment at each end.

Link to Earth Stations:

Most users cannot afford a satellite earth station, so a land line is needed for a connection to the nearest earth station (Which they tell me is 65,000 bps for a leased line). Because of the great distance the signal must travel in space, the relatively short distance between the two users on earth becomes insignificant and actually does not affect the operating cost. It is generally not economical. This is particularly true of high-capacity or broadband applications. Even though operating costs are insensitive to distance, satellite companies may still charge more for longer distances based on terrestrial line competition.

Nonterrestrial Problems:

The nonterrestrial portion of satellite communications bypasses the problems encountered with broken phone lines, etc., but it has its own unique set of problems. Since satellite communications employ high-frequency microwave radio transmission, careful planning is required to avoid interference between the satellite and other microwave systems. Eclipses of the sun, and even the moon, can cause trouble because they cut off the source of energy for the satellite’s solar batteries. Backup batteries are used to resolve most of these difficulties, but the problem that is the most severe is when the sun gets directly behind the satellite and becomes a source of unacceptable noise. This occurs 10 times a year for about 10 min each time. In order to obtain uninterrupted service, an earth station must have a second dish antenna a short distance away or the single dish antenna must have access to another satellite.

Accessing the Satellite:

There are three methods by which multiple users (earth stations) can access the satellite. The first is frequency-division multiple access (FDMA), whereby the total bandwidth is divided into separate frequency channels assigned to the users. Each user has a channel, which could remain idle if that user had no traffic. Time-division multiple access (TDMA) provides each user with a particular time slot or multiple time slots. Here the channels are shared, but some time slots could be idle if a user has no traffic to offer. With code-division multiple access (CDMA) each user can utilize the full bandwidth at any time by employing a unique code to identify the user’s traffic. There are, of course, trade-offs among the three methods; they involve error rate, block size, throughput, interference, and cost.

Advantages:

o Satellite lines are exceptionally well suited for broadband applications such as voice, television, and picture-phone, and the quality of transmission is high.
o Satellite lines are generally less expensive for all voice and data types of transmission, whether it be dial-up or a leased line that is not short. This is particularly true of overseas transmissions, and there is no underwater cable to create maintenance problems.

Disadvantages:

o The propagation delay of about a quarter second way requires the participants of a voice conversation so slightly delay their responses to make sure no more conversation is still on the way. The propagation delay has more of a severe effect on the transmission of data, and the effect becomes more pronounced with high speeds, half duplex operation, smaller blocks of data, and polling. Satellite delay units, front end processors, multiplexers, and other devices have been designed to get around these problems, but there is no solution to the half second lost in total response time for interactive applications.
o Some of the modems currently in use today have not been designed to handle the long delay of the initial connection via satellite, and the result can be a lost connection. This can be frustrating when the common carrier elects to use satellite lines for regular dial-up calls up to say, 55 percent of all calls out of a particular city during the busy traffic periods.

Closing:

Satellite communications is a very interesting topic to study. Perhaps even the present/and future satellite and Ham radio "Hackers" will one day be running a Bulletin Board off of a WESTSTAR satellite -- Who’s to say there isn’t one now? (Devious Snicker)

     --Scott Holiday

==Phrack Inc.==

Volume Two, Issue 21, File 6 of 11

```
   <><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
   <>                                                                      <>
   <> Organizations Supporting The Telecommunications Network Operations <>
   <>                                                                      <>
   <>                     NETWORK MANAGEMENT CENTER                        <>
   <>        ______________________________________________________        <>
   <>       |                                                      |       <>
   <>       | A description of the Network Management Center/NMC   |       <>
   <>       | and its role in providing the best possible service   |       <>
   <>       | to the customers of the telecommunications network.  |       <>
   <>       |______________________________________________________|       <>
   <>                                                                      <>
   <>                         Brought to you by                            <>
   <>                    Knight Lightning & Taran King                     <>
   <>                                                                      <>
   <>                          August 9, 1988                              <>
   <>                                                                      <>
   <><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><><>
```

=-=

Introduction To Network Management - Southwestern Bell Telephone Company

Modern Telecommunications Networks, relying on direct customer input and common and stored program controlled switching, are generally very reliable and have provided the means to supply low cost telecommunication service to all who desire it. Because these networks are designed on the probability that all customers do not require service simultaneously, they are engineered and equipped to provide acceptable levels of service during normal traffic load periods. When customer demands or equipment malfunctions cause a deviation from the engineered requirements or heavier than normal calling occurs, modern networks can become congested and network throughput can be affected.

Network Management provides a means to improve the
performance of the network during these contingencies.

- -

Purpose And Objectives

The Network Management Centers purpose is to provide the constant surveillance and control activities necessary to maintain the network at its optimum level of performance. This includes the Bell Operating Company (BOC) Intra-Lata Networks and Inter-Exchange Facilities and Circuits.

NMC's objective is to meet customer and market needs and expectations, and at the same time, maximize revenues derived from the provision of network service.

While the NMC cannot guarantee a certain level of service to the customer, it can ensure the most effective use of existing network capacity in all situations. This will result in:

- More completed calls
- Higher return on network capital investment
- Better customer service
- Protection of essential services such as 911, during abnormal network situations
- Ensuring equal access
- Assisting in national security and emergency preparedness

The NMC has the capability to alter or change the switching network on a near real-time basis. This is accomplished thru Network Control Actions in the switching machines. Control messages from the NMC are acted upon by the switching machines to either expand capacity by utilizing idle equipment and trunks or to restrict the network by denying access to traffic that has a poor chance of completion, thereby freeing equipment and trunks for traffic that has a good chance of completion.

- -

Principles And Responsibilities Of Operations

In accomplishing the purpose and objective of the NMC, decision on network control actions are guided by standard principle applicable to switching technology or network architecture. All network management control actions are generally based upon at least one of the standard principles.

Inhibit Switching Congestion

Large numbers of ineffective attempts in a switching machine due to traffic overload or equipment malfunctions can exceed the engineered capacity of the system. If not controlled, this congestion can spread to other connected switching systems. Network management controls are available that remove ineffective attempts to a congested machine, inhibiting switching congestion and preventing its spread to adjacent switching systems.

Use All Available Trunks

The switching network is sized and equipped to accommodate the average business day calling requirements. Focused overloads (storms, holidays, floods, and civil disturbances) can often result in greatly increased calling patterns for which the network is not designed. This aberration can also be caused by facility failures and switching system outages. In these cases some trunk groups are greatly overloaded while others may be virtually idle. Network management reroutes can be activated in many of these cases to use temporary idle capacity in the network, thereby completing calls that would otherwise be blocked.

Keep All Trunks Filled With Messages

A message is a completed call. Since the network is normally trunk limited, it is important to optimize the ratio of messages (revenue) to non-messages (non revenue producing) on any trunk group. When unusual or abnormal conditions occur in the network that cause increased short holding time calls (non-message such as busy tone, reorder tone, recorded announcement, and high-and-dry - dead air), the number of carried messages decreases because non-message traffic is occupying a larger percentage of system capacity. Network management controls are designed to reduce non-message traffic and allow more calls to complete. This results in higher customer satisfaction and increased revenue for the industry.

Give Priority To Single-Link Connections

In networks designed to automatically alternate route calls, the most efficient use of available trunking occurs when traffic loads are at (or below) normal engineered values. When the engineered traffic load is exceeded, more calls alternate route and therefore are required to use more than one trunk in order to complete a call. During overload situations, the use of more than one trunk to complete a call occurs more often and the possibility of a multilink call blocking other call attempts is greatly increased. Thus, in some cases, it becomes necessary to use network management controls to limit alternate routing in order to give first routed traffic a reasonable chance to complete more calls on the network than would otherwise be completed.

The responsibility of the Network Management Center is far-reaching, affecting many work groups and organizations both in Southwestern Bell Telephone Company, other telephone companies, and the customers.

The NMC provides:

- Real-time surveillance and control of the switching network
- Identifying abnormal network situations
- A centralized point for information to higher management, IC's, Independent Companies, and other BOC's.
- A focal point for national security and emergency preparedness concerns

- -

The System -- A Picture

The Network Management System consists of three major components: The switching network itself, the data gathering support system, and the surveillance and control system (NMC).

The NMC is driven by customer actions in the switching network which are recorded and displayed via the EADAS/NM (Engineering Administration Data Acquisition System for Network Management). Network management control actions are directed from the CRT to the switching network via the same system.

Diagram;

```
           Switching             Data Gathering        NMC Surveillance
            Network                  System               and Control
         ____________          __________________     ______________________
        /            \        /                  \   /                      \
         ____________                         ___      _______________
        |            |_______________________|   |    |               |
        |   Access   |                       | E |   /| Display Board |
        |   Tandem   |         ___           | A |  / |_______________|
        |            |        |   |__________| D | /
        | End Office |________| E | Data     | A |/
        |            |        | A |__________| S |\
        |   Equal    |        | D | Network  | / | \
        |   Access   |        | A | Controls | N |  \
        | End Office |        | S |__________| M |   \
        |____________|        |___|          |   |    \   __________________
                                |            |   |     \ |                  |
                               _|_           |   |      \| Cathode Ray Tube |
                              /   \          |   |       |__________________|
                              \___/          |___|
```

- -

Introducing: The Southwestern Bell Telephone Company
                          Network Management Centers

```
        ___________________
       |                   |
    ___| Southwestern Bell |__________________________________________
   |   |   Corporations    |          |               |               |
   |   |___________________|    ______|_______  ______|_______  ______|_______
   |                           |              ||              ||              |
   |                           |   SW Bell    ||   SW Bell    ||   SW Bell    |
   |                           |Mobile Systems||   Telecom    || Publications |
   |                           |______________||______________||______________|
 __|________________
|                   |
| Southwestern Bell |
|     Telephone     |
|___________________|
   |
   |---->   Little Rock NMC        Arkansas (Non EADAS/NM)      (501)373-5126
   |---->   St. Louis NMC          Missouri & Kansas            (314)658-6044
   |---->   Oklahoma City NMC      Oklahoma                     (405)278-5511 *
   |---->   Dallas NMC             North Texas                  (214)464-2164
   |---->   Houston NMC            South Texas                  (713)850-5662 *

                                * - After hours, this number goes to a beeper,
                                    at the tone, dial in your telephone number.
```

- -

Summary

Network Management is the term used to describe a variety of activities associated with improving network traffic flow and customer service when abnormal conditions (unusual traffic patterns or equipment failures) may have resulted in a congested inefficient network. These activities include the application of network controls when and where necessary and planning the means by which the impact of network overloads can be minimized.

Network Management is based upon the use of near real-time trunk group and switching system data and the ability to implement appropriate network controls thru the use of EADAS/NM.

Network Management is concerned with completing as many calls as possible within the Intra-Lata network and providing equal treatment for the traffic flow to and from all inter-exchange carriers.

"The Future Is Forever"

==Phrack Inc.==

Volume Two, Issue 21, File 7 of 11

```
()()()()()()()()()()()()()()()()()()()()()()()()()()()()()()
()                                                        ()
()                  Non-Published Numbers                 ()
()                  ~~~~~~~~~~~~~~~~~~~~~                 ()
()             An Observation Of Illinois Bell            ()
()                                                        ()
()                   by Patrick Townson                   ()
()                of The Portal System (TM)               ()
()                                                        ()
()             Special Thanks to Hatchet Molly            ()
()                                                        ()
()()()()()()()()()()()()()()()()()()()()()()()()()()()()()()
```

All examples in this message pertain to Illinois Bell Telephone Company, which covers the Chicago metropolitan area, and quite a bit of the rest of Illinois.

- -

There are three types of phone numbers which do not appear in the printed and publicly available directory;

(1) Too new to list
(2) Non-listed
(3) Non-published

The third category of numbers not in the phone book or available from the Directory Assistance Bureau are non-published numbers. Non-published numbers are NOT available at the directory Assistance level. Inquiries about same which are input into a DA (Directory Assistance) terminal simply come up with a message that "at the customer's request, the number is not listed in our records; the number is non-published."

Well, who does keep non-pub records then? The Business Office has no handy way to retrieve them, since they depend on an actual phone number when they pull up a record to discuss an account. Once a service order is processed, the number and associated name are no longer available to the average worker in the central office.

There was for several years a small group known as the "NonPub Number Bureau" which at the time was located in Hinsdale, Illinois. Needless to say, the phone number to the NonPub Number Bureau was itself non-published, and was only available to specified employees at Illinois Bell who were deemed to have a "need to know clearance." Now with all the records being highly computerized, the keepers of the Non-Pub phone numbers are themselves scattered around from one phone office to another.

When there is some specific need for an employee at the phone company to acquire the non-published number of a subscriber, then certain security precautions kick into place. Only a tiny percentage of telephone company employees are deemed to have a "need to know clearance" in the first place; among these would be the GCO's (Group Chief Operators), certain management people in the central offices, certain people in the Treasury/Accounting office, and of course, security representatives both from Illinois Bell and the various long distance carriers, such as AT&T, US. Sprint, and MCI.

Let us have a hypothetical example for our correspondent; Your mother has taken seriously ill, and is on her deathbed. Your brother is unable to reach you to notify you of this because you have a non-pub number. When his request for the number has been turned down by Directory Assistance, simply because they do not have it, he asks to speak with a supervisor, and he explains the problem. He provides his own name and telephone number, and the supervisor states he will be called back at a later time. The supervisor does not question if in fact an emergency exists, which is the only valid reason for breaking security. The supervisor may, if they are doing their job correctly, ask the inquirer point blank, "Are you stating there is an emergency situation?"

Please bear in mind that the law in Illinois and in many other states says that if a person claims that an emergency exists in order to influence the use (or discontinuance of use) of the telephone when in fact there is no emergency is guilty of a misdemeanor crime. You say yes this is an emergency and I need to contact my brother/sister/etc right away. The supervisor will then talk to his/her supervisor, who is generally of the rank of Chief Operator for that particular facility.

The Chief Operator will call the NonPub people, will identify herself, and *leave her own call back number*. The NonPub people will call back to verify the origin of the call, and only then will there be information given out regards your brother's telephone number. It helps if you know the *exact* way the name appears in the records, and the *exact* address; if there is more than one of that name with non-pub service, they may tell you they are unable to figure out who it is you want.

The NonPub person will then call the subscriber with the non-published number and explain to them what has occurred, "So and so has contacted one of our operators and asked for assistance in reaching you. The party states that it is a family emergency which requires your immediate attention. Would it be alright if we give him/her your number, or would you prefer to call them back yourself?"

Based on the answer given, the number is either relayed back to the Chief Operator, or a message is relayed back saying the non-pub customer has been notified. If the customer says it is okay to pass his number, then the Chief Operator will call you back, ask who YOU are, rather than saying WHO she wants, and satisfied with your identification will give you the number you are seeking or will advise you that your brother has been given the message by someone from our office, and has said he will contact you.

Before the NonPub people will even talk to you, your 'call back number' has to be on their list of approved numbers for that purpose. A clerk in the Business office cannot imitate a Chief Operator for example, simply because NonPub would say that the number you are asking us to call back to is not on our list. "Tell your supervisor what it is you are seeking and have them call us..." Other emergency type requests for non-pub numbers would be a big fire at some business place in the middle of the night, and the owners of the company must be notified at their home; or a child is found wandering by the police and the child is too young to know his parent's (non-pub) number.

They will also handle non-emergency requests, but only if they are of some importance and not frivolous in nature. You have just come to our city to visit and are seeking a long lost friend who has a non-pub number; you are compiling the invitations to your high school class fiftieth re-union and find a class member is non-pub. Within certain reasonable limits, they will pass along your request to the desired party and let them make the choice of whether to return the call or not. But always, you leave your phone number with them, and in due time someone will call you back to report what has been said or done.

You would be surprised -- or maybe you wouldn't -- at the numerous scams and stories people tell the phone company to get the non-pub numbers of someone else. Fortunately, Bell takes a great deal of pride in their efforts to protect the privacy of their subscribers.

-PT

```
                                ==Phrack Inc.==

                      Volume Two, Issue 21, File 8 of 11

          \`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\
          \`\                                                         \`\
          \`\           BLOCKING OF LONG-DISTANCE CALLS               \`\
          \`\                  by Jim Schmickley                      \`\
          \`\                                                         \`\
          \`\           Hawkeye PC, Cedar Rapids, Iowa                \`\
          \`\                                                         \`\
          \`\           Special Thanks To Hatchet Molly               \`\
          \`\                                                         \`\
          \`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\`\
```

SUMMARY -- This file describes the "blocking" by one long-distance telephone company of access through their system to certain telephone numbers, particularly BBS numbers. The blocking is applied in a very arbitrary manner, and the company arrogantly asserts that BBS SYSOPS and anyone who uses a computer modem are "hackers."

The company doesn't really want to discuss the situation, but it appears the following scenario occurred. The proverbial "person or persons unknown" identified one or more "valid" long-distance account numbers, and subsequently used those numbers on one or more occasions to fraudulently call a legitimate computer bulletin board system (BBS). When the long-distance company discovered the fraudulent charges, they "blocked" the line without bothering to investigate or contacting the BBS System Operator to obtain his assistance. In fact, the company did not even determine the sysop's name.

The long-distance carrier would like to pretend that the incident which triggered the actions described in this article was an isolated situation, not related to anything else in the world. However, there are major principles of free, uninhibited communications and individual rights deeply interwoven into the issue. And, there is still the lingering question, "If one long-distance company is interfering with their customers' communications on little more than a whim, are other long-distant companies also interfering with the American public's right of free 'electronic speech'?"

CALL TO ACTION -- Your inputs and protests are needed now to counter the long-distance company's claims that "no one was hurt by their blocking actions because nobody complained." Obviously nobody complained for a long time because the line blocking was carried out in such a manner that no one realized, until April 1988, what was being done.

Please read through the rest of this article and judge for yourself. Then, please write to the organizations listed at the end of the article; insist that your right to telephone whatever number you choose should not be impaired by the arbitrary decision of some telephone company bureaucrat who really doesn't care about the rights of his customers. Protest in the strongest terms. And, remember, the rights you save WILL BE YOUR OWN!

SETTING THE SCENE -- Teleconnect is a long-distance carrier and telephone direct marketing company headquartered in Cedar Rapids, Iowa. The company is about eight years old, and has a long-distance business base of approximately 200,000 customers. Teleconnect has just completed its first public stock offering, and is presently (August 1988) involved in a merger which will make it the nation's fourth-largest long-distance carrier. It is a very rapidly growing company, having achieved its spectacular growth by offering long distance service at rates advertised as being 15% to 30% below AT&T's rates.

When Teleconnect started out in the telephone interconnection business, few, if any, exchanges were set up for "equal access," so the company set up a network of local access numbers (essentially just unlisted local PABXs - Private Automatic Branch eXchanges) and assigned a six-digit account number to each customer. Later, a seventh "security" digit was added to all account numbers. Teleconnect now offers direct "equal access" dialing on most exchanges, but the older access number/account code system is still in place for those exchanges which do not offer "equal access." That system is still very useful for customers who place calls from their offices or other locations away from home.

"BLOCKING" DISCOVERED -- In early April 1988, a friend mentioned that Teleconnect was "blocking" certain telephone lines where they detected computer tone. In particular, he had been unable to call Curt Kyhl's Stock Exchange BBS in Waterloo, Iowa. This sounded like something I should certainly look into, so I tried to call Curt's BBS.

CONTACT WITH TELECONNECT -- Teleconnect would not allow my call to go through. Instead, I got a recorded voice message stating that the call was a local call from my location. A second attempt got the same recorded message. At least, they were consistent.

I called my Teleconnect service representative and asked just what the problem was. After I explained what happened, she suggested that it must be a local call. I explained that I really didn't think a 70 mile call from Cedar Rapids to Waterloo was a local call. She checked on the situation and informed me that the line was being "blocked." I asked why, and she "supposed it was at the customer's request." After being advised that statement made no sense, she admitted she really didn't know why. So, on to her supervisor.

The first level supervisor verified the line was being "blocked by Teleconnect security," but she couldn't or wouldn't say why. Then, she challenged, "Why do you want to call that number?" That was the wrong question to ask this unhappy customer, and the lady quickly discovered that bit of information was none of her business. On to her supervisor...

The second level supervisor refused to reveal any information of value to a mere customer, but she did suggest that any line Teleconnect was blocking could still be reached through AT&T or Northwestern Bell by dialing 10288-1. When questioned why Teleconnect, which for years had sold its long-distance service on the basis of a cost-saving over AT&T rates, was now suggesting that customers use AT&T, the lady had no answer.

I was then informed that, if I needed more information, I should contact Dan Rogers, Teleconnect's Vice President for Customer Service. That sounded good; "Please connect me." Then, "I'm sorry, but Mr. Rogers is out of town, and won't be back until next week." "Next week?" "But he does call in regularly. Maybe he could call you back before that." Mr. Rogers did call me back, later that day, from Washington, D.C. where he and some Teleconnect "security people" were attending a conference on telephone security.

TELECONNECT RESPONDS, A LITTLE -- Dan Rogers prefaced his conversation with, "I'm just the mouthpiece; I don't understand all the technical details. Our security people are blocking that number because we've had some problems with it in the past." I protested that the allegation of "problems" didn't make sense because the number was for a computer bulletin board system operated by a reputable businessman, Curt Kyhl.

Mr. Rogers said that I had just given Teleconnect new information; they had not been able to determine whose number they were blocking. "Our people are good, but they're not that good. Northwestern Bell won't release subscriber information to us." And, when he got back to his office the following Monday, he would have the security people check to see if the block could be removed.

The following Monday, another woman from Teleconnect called to inform me that they had checked the line, and they were removing the block from it. She added the comment that this was the first time in four years that anyone had requested that a line be unblocked. I suggested that it probably wouldn't be the last time.

In a later telephone conversation, Dan Rogers verified that the block had been removed from Curt Kyhl's line, but warned that the line would be blocked again "if there were any more problems with it." A brief, non-conclusive discussion of Teleconnect's right to take such action then ensued. I added that the fact that Teleconnect "security" had been unable to determine the identity of the SYSOP of the blocked board just didn't make sense; that it didn't sound as if the "security people" were very competent. Mr. Rogers then admitted that every time the security people tried to call the number, they got a busy signal (and, although Mr. Rogers didn't admit it, they just "gave up," and arbitrarily blocked the line). Oh, yes, the lying voice message, "This is a local call...," was not intended to deceive anyone according to Dan Rogers. It was just that Teleconnect could only put so many messages on their equipment, and that was the one they selected for blocked lines.

BEGINNING THE PAPER TRAIL -- Obviously, Teleconnect was not going to pay much attention to telephone calls from mere customers. On April 22, Ben Blackstock, practicing attorney and veteran sysop, wrote to Mr. Rogers urging that Teleconnect permit their customers to call whatever numbers they desired. Ben questioned Teleconnect's authority to block calls, and suggested that such action had serious overlays of "big brother." He also noted that "you cannot punish the innocent to get at someone who is apparently causing Teleconnect difficulty."

Casey D. Mahon, Senior Vice President and General Counsel of Teleconnect, replied to Ben Blackstock's letter on April 28th. This response was the start of Teleconnect's seemingly endless stream of vague, general allegations regarding "hackers" and "computer billboards." Teleconnect insisted they did have authority to block access to telephone lines, and cited 18 USC 2511(2)(a)(i) as an example of the authority. The Teleconnect position was summed up in the letter:

> "Finally, please be advised the company is willing to 'unblock' the line in order to ascertain whether or not illegal hacking has ceased. In the event, however, that theft of Teleconnect long distance services through use of the bulletin board resumes, we will certainly block access through the Teleconnect network again and use our authority under federal law to ascertain the identity of the hacker or hackers."

THE GAUNTLET IS PICKED UP -- Mr. Blackstock checked the cited section of the U.S. Code, and discovered that it related only to "interception" of communications, but had nothing to do with "blocking." He advised me of his opinion and also wrote back to Casey Mahon challenging her interpretation of that section of federal law.

In his letter, Ben noted that, "Either Teleconnect is providing a communication service that is not discriminatory, or it is not." He added that he would "become upset, to say the least" if he discovered that Teleconnect was blocking access to his BBS. Mr. Blackstock concluded by offering to cooperate with Teleconnect in seeking a declaratory judgment regarding their "right" to block a telephone number based upon the actions of some third party. To date, Teleconnect has not responded to that offer.

On May 13th, I sent my own reply to Casey Mahon, and answered the issues of her letter point by point. I noted that even I, not an attorney, knew the difference between "interception" and "blocking", and if Teleconnect didn't, they could check with any football fan. My letter concluded:

> "Since Teleconnect's 'blocking' policies are ill-conceived, thoughtlessly arbitrary, anti-consumer, and of questionable legality, they need to be corrected immediately. Please advise me how Teleconnect is revising these policies to ensure that I and all other legitimate subscribers will have uninhibited access to any and all long-distance numbers we choose to call."

Casey Mahon replied on June 3rd. Not unexpectedly, she brushed aside all my arguments. She also presented the first of the sweeping generalizations, with total avoidance of specifics, which we have since come to recognize as a Teleconnect trademark. One paragraph neatly sums Casey Mahon's letter:

> "While I appreciate the time and thought that obviously went into your letter, I do not agree with your conclusion that Teleconnect's efforts to prevent theft of its services are in any way inappropriate. The inter-exchange industry has been plagued, throughout its history, by individuals who devote substantial ingenuity to the theft of long distance services. It is not unheard of for an interexchange company to lose as much as $500,000 a month to theft. As you can imagine, such losses, over a period of time, could drive a company out of business."

ESCALATION -- By this time it was very obvious that Teleconnect was going to remain recalcitrant until some third party, preferably a regulatory agency, convinced them of the error of their ways. Accordingly, I assembled the file and added a letter of complaint addressed to the Iowa Utilities Board. The complaint simply asked that Teleconnect be directed to institute appropriate safeguards to ensure that "innocent third parties" would no longer be adversely affected by Teleconnect's arbitrary "blocking" policies.

My letter of complaint was dated July 7, 1988 and the Iowa Utilities Board replied on July 13, 1988. The The reply stated that Teleconnect was required to respond to my complaint by August 2, 1988, and the Board would then propose a resolution. If the proposed resolution was not satisfactory, I could request that the file be reopened and the complaint be reconsidered. If the results of that action were not satisfactory, a formal hearing could be requested.

After filing the complaint, I also sent a copy of the file to Congressman Tom Tauke. Mr. Tauke represents the Second Congressional District of Iowa, which includes Cedar Rapids, and is also a member of the House Telecommunications Subcommittee. I have subsequently had a personal conversation with Mr. Tauke as well as additional correspondence on the subject. He seems to have a deep and genuine interest in the issue, but at my request, is simply an interested observer at this time. It is our hope that the Iowa Utilities Board will propose an acceptable resolution without additional help.

AN UNRESPONSIVE RESPONSE -- Teleconnect's "response" to the Iowa Utilities Board was filed July 29, 1988. As anticipated, it was a mass of vague generalities and unsubstantiated allegations. However, it offered one item of new, and shocking, information; Curt Kyhl's BBS had been blocked for ten months, from June 6, 1987 to mid-April 1988. (At this point it should be noted that Teleconnect's customers had no idea that the company was blocking some of our calls. We just assumed that calls weren't going through because of Teleconnect's technical problems).

Teleconnect avoided putting any specific, or even relevant, information in their letter. However, they did offer to whisper in the staff's ear; "Teleconnect would be willing to share detailed information regarding this specific case, and hacking in general, with the Board's staff, as it has in the past with various federal and local law enforcement agencies, including the United States Secret Service. Teleconnect respectfully requests, however, that the board agree to keep such information confidential, as to do otherwise would involve public disclosure of ongoing investigations of criminal conduct and the methods by which interexchange carriers, including Teleconnect, detect such theft."

There is no indication of whether anyone felt that such a "confidential" meeting would violate Iowa's Open Meetings Law. Nobody apparently questioned why, during a ten-months long "ongoing investigation," Teleconnect seemed unable to determine the name of the individual whose line they were blocking. Of course, whatever they did was justified because in their own words, "Teleconnect had suffered substantial dollar losses as a result of the theft of long distance services by means of computer 'hacking' utilizing the computer billboard which is available at that number."

Teleconnect's most vile allegation was, "Many times, the hacker will enter the stolen authorization code on computer billboards, allowing others to steal long distance services by utilizing the code." But no harm was done by the blocking of the BBS number because, "During the ten month period the number was blocked, Teleconnect received no complaints from anyone claiming to be the party to whom the number was assigned." The fact that Curt Kyhl had no way of knowing his line was being blocked might have had something to do with the fact that he didn't complain.

It was also pointed out that I really had no right to complain since, "First, and foremost, Mr. Schmickley is not the subscriber to the number." That is true, I'm just a long-time Teleconnect customer who was refused service because of an alleged act performed by an unknown third party.

Then Teleconnect dumped on the Utilities Board staff a copy of a seven page article from Business Week Magazine, entitled "Is Your Computer Secure?" This article was totally unrelated to the theft of long-distance service, except for an excerpt from a sidebar story about a West German hackers' club. The story reported that, "In 1984, Chaos uncovered a security hole in the videotex system that the German telephone authority, the Deutsche Bundespost, was building. When the agency ignored club warnings that messages in a customer's private electronic mailbox weren't secure, Chaos members set out to prove the point. They logged on to computers at Hamburger Sparkasse, a savings bank, and programmed them to make thousands of videotex calls to Chaos headquarters on one weekend. After only two days of this, the bank owed the Bundespost $75,000 in telephone charges."

RESOLUTION WITH A RUBBER STAMP -- The staff of the Iowa Utilities Board replied to my complaint by letter on August 19, 1988. They apparently accepted the vague innuendo submitted by Teleconnect without any verification; "Considering the illegal actions reportedly to be taking place on number (319) 236-0834, it appears the blocking was reasonable. However, we believe the Board should be notified shortly after the blocking and permission should be obtained to continue the blocking for any period of time."

However, it was also noted that, "Iowa Code 476.20 (1) (1987) states, 'A utility shall not, except in cases of emergency, discontinue, reduce, or impair service to a community or a part of a community, except for nonpayment of account or violation of rules and regulations, unless and until permission to do so is obtained from the Board." The letter further clarified, "Although the Iowa Code is subject to interpretation, it appears to staff that 'emergency' refers to a relatively short time..."

CONSIDER THE EVIDENCE -- Since it appeared obvious that the Utilities Board staff had not questioned or investigated a single one of Teleconnect's allegations, the staff's response was absolutely astounding. Accordingly, I filed a request for reconsideration on August 22nd.

Three points were raised in the request for reconsideration;

(1) The staff's evaluation should have been focused on the denial of service to me and countless others of Teleconnect's 200,000 customers, and not just on the blocking of incoming calls to one BBS.

(2) The staff accepted all of Teleconnect's allegations as fact, although not one bit of hard evidence was presented in support of those allegations.

(3) In the words of the staff's own citation, it appeared that Teleconnect had violated Iowa Code 476.20 (1) (1987) continuously over a ten months' period, perhaps as long as four years.

Since Teleconnect had dumped a seven page irrelevant magazine article on the staff, it seemed only fair to now offer a two page completely relevant story to them. This was "On Your Computer - Bulletin Boards," from the June 1988 issue of "Changing Times." This excellent article cited nine BBSs as "good places to get started." Among the nine listed BBSs was Curt Kyhl's "Stock Exchange, Waterloo, Iowa (319-236-0834)." Even the geniuses at Teleconnect ought to be able to recognize that this BBS, recommended by a national magazine, is the very same one they blocked for ten months.

MEANWHILE, BACK AT THE RANCH -- You are now up-to-date on the entire story. Now, we are in the process of spreading the word so that all interested people can contact the Iowa authorities so they will get the message that this case is much bigger than the blocking of one BBS. YOU can help.

Read the notice appended to this file and ACT. If you are a Teleconnect customer, it is very important that you write the agencies listed on the notice. If you are not a Teleconnect customer, but are interested in preserving your rights to uninhibited communications, you can help the cause by writing to those agencies, also. Please, people, write now! Before it is too late!

- -

TELECONNECT CUSTOMERS

If you are user of Teleconnect's long distance telephone service, you need to be aware of their "blocking" policy:

> Teleconnect has been "lashing out" against the callers of bulletin boards and other "computer numbers" by blocking access of legitimate subscribers to certain phone numbers to which calls have been made with fraudulent Teleconnect charge numbers. Curt Kyhl's Stock Exchange Bulletin Board in Waterloo has been "blocked" in such a manner. Teleconnect representatives have indicated that other "computer numbers" have been the objects of similar action in the past, and that they (Teleconnect) have a "right" to continue such action in the future.
>
> Aside from the trampling of individual rights guaranteed by the Bill of Rights of the U.S. Constitution, this arbitrary action serves only to "punish the innocent" Teleconnect customers and bulletin board operators, while doing absolutely nothing to identify, punish, or obtain payment from the guilty. The capping irony is that Teleconnect, which advertises as offering significant savings over AT&T long-distance rates, now suggests to complaining customers that the blocked number can still be dialed through AT&T.
>
> Please write to Teleconnect. Explain how long you have been a customer, that your modem generates a significant amount of the revenue they collect from you, and that you strongly object to their arbitrarily deciding what numbers you may or may not call. Challenge their "right" to institute a "blocking" policy and insist that the policy be changed. Send your protests to:
>
> Teleconnect Company
> Mr. Dan Rogers, Vice President for Customer Service
> 500 Second Avenue, S.E.
> Cedar Rapids, Iowa 52401
>
> A complaint filed with the Iowa Utilities Board has been initially resolved in favor of Teleconnect. A request for reconsideration has been filed, and the time is NOW for YOU to write letters to the State of Iowa. Please write NOW to:
>
> Mr. Gerald W. Winter, Supervisor, Consumer Services
> Iowa State Utilities Board
> Lucas State Office Building
> Des Moines, Iowa 50319
>
> And to:
>
> Mr. James Maret
> Office of the Consumer Advocate
> Lucas State Office Building
> Des Moines, Iowa 50319
>
> Write now. The rights you save WILL be your own.

After filing a request for reconsideration of my complaint, I received a reply from the Iowa State Utilities Board which said, in part:

> "Thank you for your letter dated August 22, 1988, with additional comments concerning your complaint on the blocking of access to certain telephone numbers by Teleconnect.
>
> "To ensure that the issues are properly investigated, we are forwarding your comments to the company and requesting a response by September 15, 1988."

Again, this is a very large issue. Simply stated; Does ANY telephone company have the right to "block" (or refuse to place) calls to ANY number on the basis of unsubstantiated, uninvestigated charges of "telephone fraud," especially when the alleged fraud was committed by a third party without the knowledge of the called party? In the specific case, the question becomes; Can a long distance carrier refuse to handle calls to a BBS solely because some unknown crook has placed fraudulently-charged calls to that BBS? Incidentally, when you write, please cite file number C-88-161.

If you have any additional information which might be helpful in this battle, please let me know.

```
You can send mail to me via U.S. Mail to:  Jim Schmickley
                                           7441 Commune Court, N.E.
                                           Cedar Rapids, Iowa  52402

 (See "On The Edge Of Forever" in PWN XXI/1 for an update on this issue. -KL)
```

==Phrack Inc.==

Volume Two, Issue 21, File 9 of 11

```
    PWN PWN PWN PWN PWN PWN PWN Special Edition PWN PWN PWN PWN PWN PWN
    PWN                                                             PWN
    PWN                      Phrack World News                      PWN
    PWN                  Special Edition Issue Two                  PWN
    PWN                                                             PWN
    PWN                Created, Written, and Edited                 PWN
    PWN                     by Knight Lightning                     PWN
    PWN                                                             PWN
    PWN               Special Thanks To Hatchet Molly               PWN
    PWN                                                             PWN
    PWN PWN PWN PWN PWN PWN PWN Special Edition PWN PWN PWN PWN PWN PWN
```

Ed Schwartz Show on WGN Radio 720 AM

September, 27-28, 1988

Transcribed by Hatchet Molly

Hello. In this special presentation of Phrack World News, we have the abridged transcripts from the Ed Schwartz Show, a late night talk show broadcast by WGN Radio 720 AM - Chicago, Illinois.

The transcripts that appear here in Phrack have been edited for this presentation. For the most part, I have decided to omit the unrelated chatter as well as any comments or discussions that are not pertinent to the intent of Phrack World News. In addition to this, I have also edited the speech somewhat to make it more intelligible, not an easy task. However, the complete unedited version of this broadcast can be found on The Phoenix Project (512)441-3088, sysoped by The Mentor.

:Knight Lightning

_ _

The Cast;

A = Anna (Self-proclaimed phone phreak in Kansas City, Missouri)
AA = Sergeant Abagail Abraham (Illinois State Police; Computer Crime Section)
B = Bob (A bulletin board system operator)
BG = Bob Gates (Manager of Corporate Security for Ameritech)
CM = Chuck Moran (Director of Internal Affairs; Ameritech Applied Technologies)
D = Dan (A computer science major at DeVry Technical Institute in Chicago, IL)
ES = Edward Schwartz (Our host)
EZ = Ed Zahdi (A researcher from THE READER, a local publication in Chicago)
G = Gordon (Hatchet Molly, a graduate student at Northern Illinois University)
JM = John F. Maxfield (Our famous friend from BoardScan in Detroit, Michigan)
K = Kevin (A BBS sysop)
L = Louis (A caller)
P = Penny (A victim)
R = Robert (A legal hacker)
R = Ray (A former software pirate)
S = ?? (A consulting engineer)

Also mentioned, but not on the show, was SHADOW HAWK of Chicago, Illinois, who was recently arrested for theft of software from AT&T, and TOM TCIMPIDIS, a famous sysop who was arrested for having, unknown to him, AT&T Calling Card numbers on his legal bulletin board.

^*^

ES: It's 12 minutes after the hour. The hour, of course, is eleven o'clock. We have a tremendous amount of commerce that goes on late at night and in the early morning. When I say commerce I'm talking about computer operations of all kind from keypunching to tabulating - you name it.

We've done two programs with Ed Zahdi who is the researcher from THE READER (the weekly newspaper) from the "straight dope" column. Ed Zahdi does the research and on two appearances (on two Friday nights) within the last year or so on this program Ed Zahdi has received a number of phone calls... about computer hacking, about people whose telephones mysteriously ring in the middle of the night -- or almost any time of the day but constantly do so and they pick up the phone and there's nobody there.

The last time Ed Zahdi was on, we were flooded with calls from people who claimed that;

o There are all kinds of telemarketing people who are ringing telephones.
o That the phone company is testing phones and you don't know it.
o That the phone network gets tested every day and everybody's phone rings once or for half a ring and nobody's ever there.

I was amazed at the number and type of calls that came in. We called the phone company and we asked for some cooperation and tonight we are having as guests not only Mr. Ed Zahdi from THE READER, but also Mr. Chuck Moran, the Director of Internal Affairs from Ameritech Applied Technologies. We also have Mr. Bob Gates, Manager of Corporate Security for Ameritech.

We're gonna get into this whole thing as to whether or not people are using and abusing the phone networks. Whether or not computer hackers are ferreting out phone numbers with computers. Whether or not you can really program a computer to randomly ring every telephone in the city or not.

If you're a computer person hang around. We're also going to talk about some of the things that the phone company and other allied businesses are doing to catch up with the computer hackers.
JC: Well, that sounds interesting to me.
ES: Well now are you ready for this? The Bureau of Criminal Investigation of the Illinois State Police has a computer fraud unit.
JC: Uh-huh
ES: And do you know what they like to do?
JC: What do they like to do?
ES: Lock up computer hackers. Tonight we're going have the computer hackers running for the hills! Well maybe I should say "typing for the hills" huh?
JC: Probably! (chuckle)
ES: Because they don't run...most of them are couch potatoes.
JC: That's right!
ES: Glad to see you here Ed.
EZ: Glad to be here Ed. In In the "straight dope" we deal with all kinds of questions one of the questions we got onto was the question of ghost rings. People would hear these things primarily at night.
ES: On their home phone?
EZ: On their home phone. What would happen is that they'd be sitting at home and the telephone would ring for a half a ring or a whole ring or maybe even two rings. They would pick it up and nobody would be there. And I'd heard about this in the past. I thought it was some peculiarity of buying a phone from K-Mart or who knows where.

We got easily a dozen calls in the course of the evening from people who had the same experience happen to them. And it would always, oddly enough, happen at the same time of the night or on the same day of the week at the same time of the night and it was pretty eerie.

We got one woman, who I've spoken to several times since who said that she was an answering service operator and she had whole banks of phones and sets of these phones would jingle once at a certain time of the night and then the next day a different set would jingle at a certain time of the night and then the following week or the following whenever the pattern would repeat, but nobody was ever there. And so we decided there had to be some obvious solution to this problem and the speculation at the time was that it was some sort of a testing program that the phone company had to check out the trunk lines or something like that.

So, I called up the phone company, Illinois Bell, I called up CenTel, called up Bell Labs, called up places like that to ask if they knew anything about it. I asked whether there was a testing program, if not what explanation could they offer. They said no, there was no testing program, they had no idea. They had some speculation they thought conceivably some sort of computer ringing service was involved, but they didn’t have any really clear idea so we came back here a couple of months ago to talk about it again.

ES: We were swamped with calls again.

EZ: I asked for the woman, whose name is Pat, who was the answering service operator to give me a call. She did and she volunteered to help us out and see if we could use her phone system as a guinea pig and have the telephone company try and find out, if they had means of doing this, what the source of these ghost rings was. One of the things she pointed out was that during the Hinsdale fire or during the time that the Hinsdale switching system was out of operation after the fire there the ghost rings stopped.

ES: Ahhhh!

EZ: After it was repaired the rings started up again, but they were on a more irregular basis whereas before they were sort of like clockwork at a given time of the night.

ES: Uh humm.

EZ: Now the same sets of phones would ring on a given day, but at predictable times. And it would vary within an hour or so. So what I hoped to do at that point was to get together with Pat and try and get together with the phone company at her place and see what we could find out. Unfortunately she got sick, had a bad infection, so she was out of work for a long time.

ES: Uh humm.

EZ: She has just recently gotten back on the job and I spoke her today and our plan now is that I’ll go over to her place of business on Thursday just to see for myself and at that point I’m going to call up probably your friend Ken Went at Illinois Bell.

ES: Head of Security

EZ: We’ll see what we can find out and see if they’ll do it for cheap ’cuz we haven’t got a whole lot of resources yet. Now the problem is that the connection only lasts for a split second and I hope that they can find something out in that short of a period of time in terms of tracing but its not clear to me that its totally possible.

ES: Now one of the things that we found out when you were here a few weeks ago on a Friday night was another element to all of this. Telemarketers have been known to, in terms of getting a hold of people, ring phones of people whose numbers they don’t know.

EZ: We got some real interesting things. There were two basic theories here that I guess that I should talk about. One is that computer hackers do this. One of the things that computer hackers do is program their computers to use their modems their modems to find other computers. When they find one, there will be a characteristic tone that will tell the computer on the other end that its reached another computer. If they don’t find a computer they can disconnect real quickly before the connection is actually made and the charge is placed to their bills. So they can do this all for free basically. They’ll do this routinely to try and find new locations of computers.

ES: Right.

EZ: So that was one theory. The drawback to that theory is well, why would they do this repeatedly with a given number? Because obviously if the computer isn’t there Tuesday its not going to be there Friday afternoon. Why would they try this repeatedly every week. That was one problem. The second theory that was presented to us was that telemarketing firms do this to keep their files up to date. They want to find out if given numbers are still in use or something along those lines.

ES: Cause people do move and people do change their phone numbers.

EZ: Right, so what they do is they dial a number up real quick and hang up before you can answer it. At least they can detect whether the line is actually in use. This gives them apparently some useful information. So these were the two main theories and there were several elaborations on these that we’ll probably hear more about tonight, but those were the theories that we had. he problem of course as I say is its not clear exactly what the advantage of doing this on a routine basis, weekly or whenever would be to the person who is doing it.

ES: There there are some very important elements to all of this. First of all there was a guy on yesterday morning who apparently filed some lawsuits against companies that do telemarketing for disturbing him and he is going to set a precedent that if you are bothered at home by telemarketers that you can sue them and collect damages.

Not often a lot of money but enough to make them uhh sit up and take notice and he is trying to teach other people how to sue telemarketing people.

(Break for commercial followed by re-introductions)

CM: Thank you, Ed. It is our pleasure to be here.
ES: It’s a pleasure to have you here. Ameritech Applied Technologies is a division of Ameritech the phone company, right?
CM: Right. We’re a subsidiary of Ameritech that that deals with information technology needs of the Ameritech family which includes Illinois Bell.
ES: What are some of the things you work on or are responsible for?
CM: I’m responsible for computer security for the Ameritech companies. I also happen to have auditing for Ameritech Applied Technologies, physical security for our company. That kind of stuff.
ES: Big job!
CM: Yes. We are involved with hackers regularly all the time.
ES: Good to have you here tonight Chuck. Also I would like to introduce Mr. Bob Gates, manager of Corporate Security also with Ameritech Applied Technologies.
BG: Good Morning.
ES: And a good morning to you. Bob previously was a police officer. You have been in Corporate Security at Ameritech for how long now Bob?
BG: Since divestiture which was in January 1984. Its a much more specialized field and you deal with one particular aspect of the whole scenario.
ES: Is it correct, are our callers correct? Do you ring people’s phones at various hours of the day and night? Are there "ghost" rings? Are there people out there playing around? Is it the phone company or is it others? What’s going on?
CM: Well, I’ve been in this telephone business for 22 years now.
ES Okay now this is the Director of Internal Affairs for Ameritech Applied Technologies, Mr. Moran, go ahead.
CM: In my days at Illinois Bell, we very often heard these complaints. We kept trying to find out what it was some of the things the we’ve discovered is the computer hackers! They love to scan a prefix and look for a computer tone. They want a computer to talk to, so it’ll ring a phone. Their computer will ring your phone.
ES: Now this can be done from the bedroom of a thirteen year of a computer phreak right? Or anybody else for that matter.
CM: If he has got a semi-good computer mind he can do it while he is asleep. He can program his PC to use his modem to dial your number.
ES: Is most of the computer hacking and unauthorized use of computers done in the off hours? In other words its not people in business during the day, right? Would that be basically your computer hacker description?
CM: People still have to live, they still have to have jobs to feed themselves, and they still have to go to school or go to classes and so your going to find that since hacking is a hobby, it is going to done during their free time. Which is typically evenings, weekends, and vacation periods.
ES: I guess what I’m getting at here is I’m trying to establish most of the the computer related misbehavior comes more from private homes than from business offices.
CM: No. The studies seem to indicate that 80% of computer abusers are in fact people in business and are abusing their own company, but that is not going to cause your phone to ring. The people who are using the network to call and look for computers are the people which we typically call hackers, which amount for 15-25% of the computer abuse that goes on in the world.
ES: How concerned is Ameritech and the other technology and phone companies around the country about all of this?
CM: Well just as any business Ameritech is highly dependent upon information systems to survive. So we are concerned with whatever risks go with computer usage.
ES: Did you both see the film WarGames with Matthew Broderick?
CM and BG: Yeah.
ES: Now while the plot is pretty far-out, the theory is workable, correct?
BG: The natural inquisitiveness of the youthful mind, the need to explore.
ES: We’ve heard stories about computer hackers who have gotten into computers in government offices, high schools, colleges, and universities. They’ve

changed grades, added and subtracted information from formulas, and done all kinds of things.

Payroll records have been changed and we’ve got a thing now called the computer virus. We’ve got a conviction of a guy who is going to jail for literally destroying a computer program two days after he left the company and apparently that is something that computer people are very worried about.

Are we going to end up with a huge number of people called "computer police" here at some point? To get a handle on all of this, is that what we need?

BG: I think computer security is just a natural extension of using your computers to ensure that they are used in a secure manner. That they aren’t tampered with and they aren’t abused. To do that you have to take some degree of effort to protect your computer system.

ES: Is law enforcement geared up to deal with the kinds of crimes that you guys are working on, investigating and trying to deal with?

BG: Law enforcement does have experts with them. They also have to investigate everything else that occurs. So it becomes a priority item to private companies to make a commitment to look at it themselves to protect their systems and include law enforcement if appropriate.

ES: Is there a naivety on the part of a lot of people that just left computer systems unguarded.

BG: Yes. In reference to the law enforcement, in our current criminal justice system I know that in the states that we deal with and the federal agencies that I have dealt with part of the problem is finding a prosecutor, a judge, and a jury that understands what a computer crime is, Because they are not computer literate.

ES: Well stealing information and stealing time are crimes. How about the stories of computer hackers breaking into computers at nuclear laboratories like Lawrence Livermore Laboratories in California. This is where they do the research on nuclear weapons and God knows what else. Think of the potential of this kind of misbehavior it’s frightening.

BG: That’s why computer security has become a hot job.

EZ: I’m still trying to focus on my immediate problem here which was the question of the ghost rings. What I’m hearing you say is that you think that the ghost rings are primarily the work of hackers.

CM: I think its a very plausible cause.

EZ: The question that people raise about this of course is that you can see it happening once in a while, but why all the time on a regular basis?

CM: The computer hacker scans prefixes and will set his dialer look for computer tones. He may find a few numbers and tell two or three friends. Those two or three friends will now tell two or three other friends. They will see these numbers and then they will go and scan that whole thousand number group again.

EZ: I still don’t quite see why the ghost rings occur at exactly the same time all of the time.

CM: I can’t answer that.

ES: I respond to that by saying the times are most likely approximate. Most people’s watches aren’t perfect and neither are their memories. However if the majority of the hackers are in high school, then they are probably going to sleep at about the same time every night and setting their dialers to run while they are asleep, therefore hitting the same numbers at roughly the same time every night.

Is it correct to say that they can program these computers to do this work without any billing information being generated? And how can they do this? Or is that an area we should stay away from, I don’t want to compromise you guys.

BG: You’re talking toll fraud and that’s really not my area of expertise. Toll fraud is a fact of life, but I’m not a toll fraud person.

CM: The presumption is that the billing doesn’t kick in for a split second after the phone is picked up and that is what enables these guys to get away with this.

BG: Talk to Ken.

ES: Ken will tell you things that you’ll never be able to talk about on the radio or write about I’m afraid. We’re going to get into some other elements of all of this. Are the penalties for computer hackers set to meet the crime these days? I mean do we catch many of them do they get punished and does the punishment fit the crime?

CM: The computer hackers that usually get caught are juveniles, which means the most you can do is keep them in jail until they are 21 and confiscate their computer equipment. The U.S. Attorneys Office in the Northern District for Illinois did in fact return a juvenile indictment against a hacker who used the code name SHADOW HAWK. It made the front page of the Chicago Tribune.

ES: What did he do? Can you tell us?

CM: According to the Tribune, he stole software from AT&T.

ES: This proves that as smart as some of these hackers are, some of them get caught, maybe even a lot of them get caught. So as hard as they're working to defy the system apparently you people are working from inside the system to foil what they are doing and catch them.

CM: Exactly

ES: If you don't prosecute them when you catch then then it will not mean a thing so does that mean that the various phone companies and their subsidiaries have got a very serious mood about prosecuting if you catch people? Is that the way of the future?

CM: Every case is different. Prosecution is always an option.

ES: Are we a couple of years late in dealing with this problem?

BG: The laws typically catch up to the need. You have to identify a problem before you can really address it.

ES: We have made arrangements thanks to our guests tonight to speak to an Illinois State police detective sergeant who works on computer fraud; Sergeant Abagail Abraham.

AA: Good morning I appreciate being here.

ES: Have you been listening to the radio prior to our call?

AA: I've been glued to the radio yes.

ES: Okay. Your unit is called Computer Crime Section?

AA: Sure.

ES: How long have you been in existence?

AA: Since February 1986.

ES: There obviously was a need for it. Do we have enough state laws or state statutes for you to do what you have to do?

AA: I think so. At the time that the section came into existence, the laws were not very good. Most computer crimes were misdemeanors until a few months later when the attorney general held hearings in which we participated and thus they drafted a law.

ES: Sergeant, is it handled better at the state level as opposed to the federal level? The gentlemen here from Ameritech mentions that the US Attorneys Office has recently brought a prosecution here in Northern Illinois. Is his office going to be doing much more of this or do you see it being done at a state level?

AA: I think it depends upon the kind of case. Certain cases are probably better handled at the federal level and certain cases are handled best at the local. When dealing with the federal agencies, the jurisdiction for computer fraud is shared between the FBI and the Secret Service. So it depends upon the nature of the case as to which agency would take it, but many cases are not appropriate for the federal government to take part in.

ES: Let's say we have a student who changes a grade in a school computer system. That would be more a state case I would presume than a federal case right?

AA: Certainly it would be likely to be a state case, we had a case like that.

ES: If you were able to develop a case like that and have evidence, are you liable to get a conviction? Our guests were saying that the courts don't necessarily understand all of this. When you go into state court on this kind of a thing are you getting judges and/or juries who understand what you're talking about?

AA: Well we have had no cases go to jury trials. As a matter of fact, no cases have even gone to bench trials because as like the vast majority of cases in the system they are plead out.

ES: They plead guilty?

AA: We have a 100% conviction rate.

ES: Really!

AA: Our success is based very good cooperation from state's attorneys offices. We've had no problems bringing our cases to them.

ES: Your data is so good that by the time you make your pinch there is no way they can talk their way out of it. You've got them dead to rights.

AA: Yeah, we haven't had a problem with that.

ES: What kind of penalties are you getting Sarg?

AA: All of our cases have had a 100% conviction rate, be we haven’t had that many finally adjudicated. They are in various stages because the law is so new.

ES: I presume that you’re going to continue working very hard put more people in jail.

AA: Yes, it’s a growth industry.

ES: Is Director Margolis supportive of what you are doing?

AA: I think so. Our unit came into existence under the prior director, Zegal, but Director Margolis has been very supportive of our efforts and I suspect that he will become even more so.

ES: Do people who are victims of computer crime know who to report it to? If you operate a business and your computer has been violated or anything at all has been done to you, does the average computer owner know who to report it to?

AA: No. That’s a really easy question!

BG: I would, but only because I’m in the industry. However, the average small business man would probably be somewhat at a loss.

AA: He might not even realize that is is a crime.

BG: That’s exactly true and fortunately Illinois has had the foresight to put together a unit such as the Sergeant’s.

ES: Let’s say there is a medium size company that uses computers. I’ll invent a company. My name is Mr. X and I own a a fairly nice real estate company in the neighborhood of Chicago. I’ve got maybe a dozen employees and a couple of years ago we went to computers to keep track of our listings, and all of our accounting and our bookkeeping, our past customers, and all our contactees. I mean we’ve got a lot of data. We communicate with some other real estate agencies and so we use modems, telephone lines and let computers talk to computers. Since some of this work is done when our office is closed, we leave our system hooked up. I came in yesterday morning and low-and-behold somebody got into our computer and erased all of our data, or part of it, or changed something. I am the victim of a crime should I pick up the phone and call the Illinois State Police

AA: Sure.

ES: You’ll show up and you’ll investigate?

AA: Sure.

ES: Okay.

AA: There are several ways in which a case can get to us. One of them is that you as the victim could contact us directly and another way would be to contact the local police and hope that they would call us.

ES: There’s the key word...hope. Does the Chicago Police, the Wilmette police, the Joliet police, do they know enough to refer these cases to you?

AA: I don’t know if Joliet does, but Chicago and Wilmette certainly do. For any of the police that are out there listening at this point let me add that if we were to get a case referred to us, we will handle the case in any one of a number of ways. If the local agency brings it to us and wants nothing to do with the case because they have too much on their own we will take the case over. If they would just like to either work cooperatively or have us go with them on an interview or two to translate what the victim may be saying we’d be happy to do that too. So we have enough work to do now that we need not take cases over. We are happy to work with any agency.

CM: I think one thing worth pointing out here is that we’re focusing on on a crime via telephone. Computer crime is done from afar where the victim doesn’t know the offender.

AA: That’s true.

CM: The majority of cases probably don’t involve telephones at all. They involve companies’ own employees who are committing what amounts to embezzlement using computers. Either transferring money by computer to their own accounts or somehow playing with the books and the employer might not realize for a long time until some auditing process occurs that the crime has even occurred.

AA: You’re right. There are a number of cases like that. What happens very often in a case like that when it is somebody in-house is that the company will choose to not call it to the attention of the police they will choose instead to take disciplinary action or fire the person. Their argument most times is that they don’t want the embarrassment. We do not go out and seek headlines unless our victim is interested in having headline sought. We don’t choose to publicize cases and embarrass our victim. The stuff is simply not reported that much.

EZ: I was talking to a computer consultant once who said that the higher you are up in the company if you’re involved with something like this the less likelihood there is of not only you never doing time, but even getting any sort of penalty involved. I was there was one particular case of a guy who was an executive vice president for a bank who I think stole some phenomenal amount of money was in the millions who was discovered after some period of time and they didn’t want it to get out that one their trusted employees was a crook so they gave threw this guy a retirement banquet

ES: Hahahahahaha.

EZ: They retired him from the company and he left with honors.

AA: I like this....

EZ: The consultant said he was there and it was the most hypocritical thing he ever saw, but they will do it to avoid the unfavorable publicity.

ES: I believe it.

AA: Certainly if you are high in the organization and you control things then you can control various procedures so that you are less likely to be caught and you are probably in control of enough money that you are able to come up with creative ways to embezzle it with less suspicion aroused. I’m not sure why, but the more money you take the less likely you are to get prosecuted.

ES: People admire these kinds of crime.

(Commercial Break and then reintroductions including...)

ES: I want to welcome a new player to our game tonight, Mr. John Maxfield. John Maxfield owns a corporate security consulting company. John...are you there?

JM: Yes I am, good morning.

ES: Good morning I guess you are outside of Chicago and are you close enough to have been listening to our program?

JM: Well ahhhhh, unfortunately ahhhh I’m ahhh a bit to the east of you and I had a little trouble listening in on the radio so uhhh I’ve been listening the last few minutes on the telephone.

ES: We’ve gotten into all kinds of data here. Have you and the sergeant ever talked before?

JM: I don’t believe so. I may have talked to somebody in the Illinois State Police ummmm maybe a year or so ago, but it was not the sergeant.

ES: Sergeant Abraham you’re still there, correct?

AA: Yes. I’m here

ES: I presume John that you know Chuck Moran and Bob Gates.

JM: Yes I ahhh am acquainted with ah Bob Gates.

ES: What does a private computer security company do?

JM: Well uhhh we get involved with ahhhhhh ahhhhh the cases that perhaps don’t make the headlines. Ummmmm and my role is more of kind of in counseling clients as to how they should secure their systems and to acquaint them with the risks and the kind of the nature of the enemy what they are up against.

ES: We were talking earlier about a movie called WarGames which I’m sure you must be familiar with. My guests have been telling us a little bit about some of the things that go on. I suspect that the computer hacking problem and related behaviors is probably very severe isn’t it?

JM: Yes ahhh it certainly is a growing problem The movie WarGames kind of put out into the public eye what had been going on very quietly behind the scenes for a number of years. And uhhh of course as a result of WarGames I think there was an increase in hacking activity because now a lot of the uhhh hackers suddenly realized that it was something that maybe something they should do and achieve notoriety.

ES: I have a question here that may or may not have an answer. Why is that the legitimate use of the computer isn’t enough to satisfy its user or owner. In other words, why hack? Why misbehave? Why break the law? Why cost people a fortune? I mean there are so many fascinating things you can do with a computer without breaking the law why are so many people into this anti-social, anti-business behavior?

JM: Well that’s a difficult question..ahhhhhh you could say "why do we have criminals?" You know when you know there’s plenty of gainful employment out there. Ahhhhh the thing with the computer hackers uhhh most of them are thrill seekers. ahhh they are not the kind of people that are going to be ahhhh good achievers with computers they’re really only know how to do the destructive things. They’re kind of the analog of the vandal. Ahhhh they’re not really ahhh some of them are very bright but they’re very misguided. Misdirected. And uhhh it’s it’s kind of hard to make a generalization or a stereotype because they do kind of cover a wide spectrum. We’ve got a one end of the spectrum a lot of these young kids ahhh teenagers. And they mostly seem to be boys there is very few female hackers out there.

ES: really?

JM: Yeah that’s an interesting phenomenon. I would say that maybe there is one girl for every ten thousand boys. But ahhh anyway at the one end of the spectrum we have these kids that are just kind of running loose they really don’t know how to do very much but ahhhh when they do manage to do it they do a lot of damage. Just by sheer numbers. And then on the other end of the spectrum you perhaps got a the career criminal whose chosen to commit his crimes over the telephone line. Instead of you know holding up people with guns uhhh he robs banks by telephone. So you’ve got this wide spectrum and it’s very hard to put a stereo type to it, but most of the hackers start out because there’s kind of a thrill there’s sort thrill of ripping off the phone company or breaking into a bank computer and destroying data or something. There’s a ahhhh kind of a power trip involved.

ES: Now what you’re trying to do is advise your clients how to avoid this before it happens. Do most of them end up getting burned before they come to you or are people smart enough to invest early?

JM: Security unfortunately in the business world tends to take kind of a back seat because it doesn’t generate profits, it doesn’t generate any revenue. It’s an expense uhhh if if you’re worried about burglars and you live in a big city like I do or like Chicago. Then you know you’ve got to spend extra money for locks and burglar alarms and it’s a nuisance you’ve gotta unlock your door with three different keys and throw back all these dead bolts and stuff and turn the burglar alarm off and back on again when you leave so it’s a big nuisance. So security tends to be left sort of as the last thing you do. And uhhh of course after a corporations been hit their data’s been damaged or stolen or destroyed or whatever. Then they can’t spend enough money, you know, to keep it from happening again.

ES: We have been told there is not premise that is burglar proof, there is no person regardless of their importance in this world who is totally protectable. Is a computer or a computer system totally protectable? I mean can you teach somebody how to secure the system so the hacker just can’t get at it?

JM: Quite frankly you’re you’re correct. I think the only secure computer is one that is unplugged. Or you change all the passwords and don’t write them down so no one can log on. Like any other form of security if you put enough locks and bars on your doors and windows the burglar’s going to go somewhere else where its easier pickings. The same is true with computer security. You can secure your system from all but the really ummmm you know intense organized attack. Now obviously in industry we’ve got certain segments that are targets, if you will. Banks obviously are a target, that’s where the money is.

ES: If computers are so capable and so smart, can’t we say to a computer "Okay Computer, protect yourself"?

JM: The computer actually is fairly capable of defending itself, the only problem is it’s not intelligent. Uhh and it doesn’t really care you see whether somebody breaks in or not. You see there’s no human in the loop, if you will. So you have to have you have to have a human someplace that looks at the exception report that the computer generates and says "hey! What’s all these two o’clock in the morning logons...those accounts are supposed to be active at that time of night." Now you can program a computer to do some of that, but you still need a human auditor to scrutinize the workings of the system ever now and then just to be sure that the computer is protecting what its supposed to protect.

ES: John, what’s the name of your company?

JM: My company is called BoardScan and we’re in Detroit Michigan

ES: We have some callers, first up is young lady by the name of Penny. Are you there Penny?

P: Yes I am Ed, how are you?

ES: Good. Are you enjoying the program?

P: Yes! I’m a victim!

ES: A victim! Tell us how.

P: We moved in about three months ago, two of our phones are rotary service and one of them is a cheapy touch-tone that you go from touch to pulse or something on it. When somebody dials out on one of the rotary phones, this cheapy phone beeps back at us. Well I don't mind it too much because I've got little kids and I get to know who's using the phone. Except, 10:38 at night when my kids are sleeping and I'm sitting in the family room, my little touch-tone phone beeps at me. Twice.

JM: Oh I think I can explain that, perhaps. Now it just beeps...

P: Twice!

JM: It does it every night about the same time?

P: Just about, yeah.

JM: Well there's an automatic scanner in every telephone exchange that runs at night testing lines.

ES: Oh no! Now wait a minute!

P: Now wait a minute! They said that doesn't happen! No no no no.

ES: The phone company all right. This is the one thing that everybody we've talked to in the telephone industry has denied!

EZ: We, ahh, yeah....

ES: Go ahead Ed! Take over, take over

EZ: We talked to a number of people at the phone company and the original thought was the phone company was doing some sort of testing, but the people at the phone company we talked to said "no...they don't." That testing occurs only when the actual connection is made in a routine phone call. This is part of the on-going sort of testing program. There is no additional testing, however, they said. Now does it work differently in Michigan?

JM: Well I don't know. I know I have a phone that ahhh will ahh...it's got like a little buzzer in it and it will go "tick- tock" at about 1:30am every night. And ummmm if you're on a if you're on one of the older electro-mechanical exchanges uhh then I dare say there is a scanner that does scan all the lines at night. And it it only stops on each line for about oh a 1/2 second...just long enough to make your phone go beep-beep. And I'm sure that's what the explanation is. I am pretty qualified, before I got computer security work I used to install telephone exchanges.

P: Okay, I have a home computer. It's a Commodore I do not have a modem. Is there anyway that I could get one and verify this?

JM: Ahhhhh I don't what a modem would have to do with the telephone company testing your line at 10:30 at night. I don't see the connection there.

P: What would verify it? Could I verify that I'm being used as a test or would it verify that I'm being scanned by some other computer someplace?

JM: Well no. If you were being scanned by a hacker, you'd be getting an actual ring, you wouldn't get just say a short beep.

EZ: Penny where do you live?

P: Oaklawn.

EZ: Would you be willing to participate in a little experiment?

P: Sure, it happens pretty regularly.

EZ: Okay. Well is it every night or just some nights?

P: 6 nights out of 10. More than 50-50. It happened tonight as a matter of fact.

EZ: Okay well tell you what.

P: It happened last night as a matter of fact!

ES: Penny, we'll get your name and your number and Ed is going to call you during the day and do a little work with you, okay?

P: Sounds good.

ES: Thanks Penny. Hold on a minute okay?

P: Thank you.

ES: You see now, Mr Maxfield is telling us something that every source we've gone to has denied. There's no such thing they tell us as of random testing of the phone network either by the local phone company or by AT&T they say to us "what for?" There's no need to do it. There's no reason to do it. Let me ask our guests in the studio here from Ameritech. Has either one of you ever heard of anything like this? Is it the kind of thing that either one of you can address? I know that you're computer guys, but what about this?

CM: I know who you've talked to over at Illinois Bell Security and at one time historically they used to do testing, but they stopped that when I was still at Illinois Bell.

ES: So this is some years ago.

CM: Yeah.

EZ: Now did it only apply to the electro-mechanical systems?

CM: The only offices I ever worked out of were electro-mechanical, so yes.

JM: Well I don't know. That would be my first guess because I know when I was on electro-mechanical exchange here in Detroit that's what would happen every night.

ES: It’s a different phone company.

JM: Well I know, it’s the same equipment though. Now on two electronic switching systems the line is tested every time you make a call. So there isn’t any scanner like that. I think the mystery would be solved by just verifying what kind of equipment you know she was being served out of.

EZ: It never dawned on us that that would make a difference.

(Commercial Break and then reintroductions including...)

ES: I’ve got a call coming in here long distance from Missouri. Anna are you there?

A: Yes I am.

ES: Where in Missouri are you?

A: I’m in Kansas City.

ES: And you’re listening to us tonight?

A: Yes.

ES: Okay now my producer tells me that when you called up you identified yourself as a computer hacker, is that correct?

A: I am a female phone hacker and computer hacker, Yes.

ES: One of the few because apparently mostly males are into this.

A: Uh-huh.

ES: Anna, talk up a little bit louder. How old are you?

A: I’m 27.

ES: Twenty seven years old and do you have a job?

A: No.

ES: You don’t?!

A: No I have a lot of idle time.

ES: And you’re a computer hacker. By definition what do you do with your computer that makes you a hacker?

A: Well I scan out codes that residents and companies have with US Sprint and different companies and I’ve used about fifteen thousand dollars worth of free long distance.

ES: Are you calling free right now?

A: Yes I am. I am not paying for this call.

ES: Your computer has allowed you to make an illegal long distance call?

A: Through the computer I obtain the codes and then I dial codes with the touch-tone.

ES: Sergeant, should I be talking to her since she’s committing crime right now. Am I aiding and abetting her? No wait..no. I’ve got a police officer on here....Sarge?

AA: Yes.

ES: What do you think? Should we continue with this?

AA: I’d be real curious to know what her justification is for her behavior.

ES: How about that Ann, how about giving us an answer for this?

A: Well I have a lot of idle time and very little money and I like to talk to a lot of my friends. I have a suggestion for companies and residents out there who might have remote access codes. You might make them difficult, not not easy where hackers could, you know the first things they try are like 1-2-3-4, etc.

ES: Well let me ask you a question Anna. Have you found your computer hacking to be relatively easy to do?

A: Yes I have.

ES: So you’re saying that the computer people of the world have not tried hard enough to keep you out?

A: No they haven’t. I would suggest as far as the phone companies who use remote access codes to make the codes more difficult.

ES: When we run into people like Anna who obviously have some intuitive talent and some success at this, why don’t we hire some of these people and put their knowledge to work?

AA: No!

ES: No?

JM: No. No. I’d have to say no to that also.

A: Why not?

JM: You have to understand the the technical side of it. Just knowing how to hack out a code doesn’t qualify you as knowing how to change they system so you can’t hack codes anymore.

AA: There’s a perception that these people are all whiz-kids and I don’t think that’s the case.

ES: Are you a whiz-kid Anna?

A: No, I don’t always use the computer to find these codes I have a lot of friends and I also do some hacking of my own and there are a lot of different methods. What you figure out is what how many digits are in the codes and different things like that so it does require some brains. Unless you have friends of course and that’s all you rely on.

ES: Do you not understand that what you are doing is illegal? Does that not even enter into the equation?

A: Of course I understand that! Yes.

ES: That what you are doing somebody else ultimately has to pay for Doesn’t that bother you? I mean if you were the victim of a thief or a burglar, I presume you would call the police and you’d scream and yell until they did something about it. And yet you and so many thousands of other people think nothing of committing thievery and fraud by wire and God knows what other crimes and because your victim is not sitting in the same room with you it just doesn’t seem to bother you.

A: Well I haven’t I haven’t physically bodily hurt anybody and it’s mostly companies you know that I’ve dealt with.

ES: That makes it okay? Companies are made up of people. Sometimes they’re privately owned and sometimes they’re made up of stockholders, but companies are people and so you’re hurting people.

CM: I don’t know what service she’s coming through on, but you gotta remember its costing that company money right now to enable her to talk and they’ve got to recover those costs from their legitimate customers.

A: Don’t they just use it as a tax write-off?

BG: No.

JM: There’s been some of the smaller long distance companies, some of the people that resell service provided by AT&T or Sprint, some of these smaller companies have actually been bankrupted by people like Anna.

A: Well I happen to know the person who bankrupted one of them.

AA: I don’t see why that’s something that would make anybody proud.

A: I’m not proud to know this person.

AA: Why would you be proud to do what you’re doing because you’re doing the exact same thing, just perhaps not at the same scale.

A: Well I don’t I don’t deal with small time companies.

AA: So, you and many people like you are costing large companies a enormous sum of money. You’re the people you’re the reason that a company like Sprint is not profitable and could in fact bankrupt or could have to lay people off and could put people out of work.

A: They’re not profitable?

JM: Sprint has been losing money almost since the beginning.

CM: Or just make a basic rate increase which makes phone service less affordable.

EZ: My long distance company is All-Net which has had to change access codes three times in the last year. Primarily because of hackers and I don’t think it’s ever been profitable.

CM: Which is inconvenient to you as a customer.

EZ: Sure

ES: I think what bothers me the most out of this whole thing with Anna is the fact that she is, committing crime literally every day and just doesn’t acknowledge that as either morally offensive.

JM: Yes you’ve hit on the crux of the problem here. Ahhh these phone phreaks and hackers really don’t see themselves as criminals and the crime here is totally anonymous it’s as simple as dialing some numbers on a telephone that belong to someone else. Okay and so there is no victim. I mean the hacker or the phone phreak doesn’t even know the victim that ahh they’re billing the call to. In most cases.

ES: Like the burglar who burglarizes during the day when nobody is home he doesn’t see the faces of his victims and so its a very impersonal crime. Anna how would you feel if someday you get a knock on the door and it’s the FBI or the Secret Service and they have finally tracked you down and the US Attorney for Kansas City decides to indict you and they’ve got a good case and you end up going to prison. How would you feel then?

A: My original reason for taking an interest in this particular hobby is that someone got hold of my AT&T calling card and ran up my phone bill to several thousand dollars and I took an interest in it to find out originally what was going on with it. Now I have had contact with the Secret Service and the FBI and they didn’t do anything about the person who offended me. They didn’t do anything at all.

AA: That doesn’t answer the question.

ES: Well what’s going to happen if they come back and grab you? How would you feel if you ended up having to go to prison?

A: I guess those are the breaks.

ES: Are you married or single?

A: I’m single.

ES: Does your family know that you’re involved in all this?

A: Yes they do.

ES: I mean how would they react if you ended up being arrested?

A: I guess they wouldn’t get anymore free long distance.

ES: They’re using it too!?

A: They have me place the calls for them.

ES: You know what disturbs me. You know don’t sound like a stupid person, but you represent a lack of morality that disturbs me greatly. You really do. I think you represent a certain way of thinking that is morally bankrupt. I’m not trying to offend you, but I’m offended by you!

A: Well I appreciate your time and you giving me air time an everything. I thought I’d let some of you know that we are out there and look out for us. Change those remote access codes to more difficult codes and...

BG: Is that to make the challenge more difficult for you?

A: Possibly for some of us, but to also those hackers who don’t have the intelligence or don’t have the friends or don’t have the computers or whatever they’re using.

BG: Or the idle time.

A: Right, the idle time. There you go.

ES: How do you pay your rent Anna? Or do you live at home with your folks?

A: I live with my parents.

ES: Oh...okay.

AA: Why not take that time and do something constructive or socially useful?

A: Well I went out and applied for a job with US. Sprint and didn’t get hired.

AA: That’s good!

EZ: Is it any wonder?!

ES: Anna, do you listen to this program very often? I don’t believe you’ve ever called before have you?

A: No.

ES: Do you listen every once in a while?

A: Yes. I had just happened to hear through a friend that it was coming on.

ES: Okay. I tell you what Anna. A little something for all new callers. I’ve got very fancy WGN T-shirts. If you give my producer your name and address we’ll send one to you. Okay?

A: Okay

ES: We’ll be right back. (Click!) She hung up. I have to tell you the truth. I thought we had her there for a minute.

AA: Well done!

JM: She hung up on you?

ES: The minute we went in on the line to get her address to send her the prize she hung up.

JM: Yeah, I don’t doubt that.

ES: I’m not trying to make an enemy out of the woman, but I really am disturbed by her lack of moral fiber. I got another person on the phone claiming to be a computer hacker. Dan, are you there?

D: Yes

ES: Are you a computer hacker?

D: No. I’m a computer science major.

ES: Oh, okay.

D: I’d like to ask your security experts what types of risk avoidance is involved in providing unauthorized people into corporation’s computer systems?

BG: What you’re asking us is what we do to try to keep unauthorized people out and for me to answer that, would give away the store.

AA: Besides it would take about two days.

JM: I think you can answer that in generalities. As a number we’re talking about I guess, telephone dial-up access to computers.

BG: I think he’s asking generically. Just computing. I don’t think it would be appropriate for me to discuss. There is enough literature out there, you’re a computer science major you read the literature and I think your answer lies there.

EZ: Just to give you an example I know in terms not so much as computers, but misuse of long distance credit card numbers, the All-Net people who I deal with made their numbers longer which is the simplest thing you can do. It’s harder to find one that’s working.

JM: When protecting your computers, the first line of defense is the password.

Obviously you don’t want to use trivial passwords. Ahhh that’s the first line of defense. After that you add on other things like dial-back, encryption and various other techniques to rule out anyone with just a casual ahhh attempt at access that is just not going to get through.

ES: Dan, where are you going to school?

D: Right across the street from WGN, the Devry institute.

ES: What is your feeling when you hear somebody else talk about, you just heard Anna, what what’s your feeling about what she’s doing?

D: I’m not really familiar with the hackers.

ES: Don’t you see things being stolen? Does that bother you at all? I mean you see the illegality of it? The immoral...morality of it?

D: I think it’s very unethical because a lot of the companies have billions of dollars in equipment.

ES: It’s not something you’re into? Correct?

D: That’s correct, yes.

ES: I’m glad. Thanks for your call Dan.

D: Okay.

ES: Hello Louis are you there?

L: Yes I’m here.

ES: Okay you’re on with all of our panel members Louis.

L: Thank you very much. I heard a story that had to do with a certain hacker who had gotten inside the computer system of a let’s say a large oil company. We’ll leave the names out of it. They had set up a security system which automatically traces the call directly back to wherever the originating connection is made and this goof called from his home. Two or three days later, he found FBI agents on his front door step.

AA: I’m not familiar with the case, but it’s certainly is within the realm of possibility.

JM: This happens quite a bit. A person like Anna for example might use a long distance service that is subscribing to a service from the originating telephone company of identification of calling number. When the fraudulent bill is generated the number that placed the call is also there and working it backwards is very trivial at that point.

L: They simply did something like putting a trap on the line.

JM: On some of the systems, the trap is already there. It’s just part of the system, it’s not really a trap at all.

ES: There are ways to catch people and the computer hackers like to play the odds. All right Louis thank you.

L: Hopefully this will teach a lot of people who are considering doing something like this to keep their hands off.

ES: I hope so, good point. Thanks for the call.

L: Thank you very much

ES: We’ve got a call here. Hello Bob!

B: I’d like to make a few comments on computer law. I live in Oaklawn and they’ve got the most modern exchanges that Illinois Bell has to offer. My son lives in that area and I know they offer features that are only available on the newer switches out there. I go back with computers to before Apple and IBM sold PC’s, I had a couple sitting here at home.

ES: Uh-humm.

B: I bought my first modem about 1978. I consider myself somewhat a hacker, but I’ve never really tried to get into anybody else’s system, not so much that I considered it illegal, simply because there wasn’t that much of interest to me available. As far as computers go, if I sit here and dial random phone numbers in some states, now that is illegal. It’s illegal if your 14 year old is sitting at home at a computer, but it’s not illegal if your using a computerized phone system for generating sales leads.

ES: We call it tele-marketing.

B: Tele-marketing is essentially what some hackers have been hassled for and n some states it is illegal now. I’ve accidentally accessed systems I did not intend to access.

CM: You didn’t pursue that right?

B: No, I’ve never used it. I’ve never used a computer for theft of services. I am not about to try and defend somebody that uses a computer to as a tool for theft of service from a telecommunications company. However, there are certain computer laws that never should have been passed. The case of the fellow out in California two or three years back that had a bulletin board, somebody had posted access codes on his bulletin board. He has an automated machine that answers his telephone. The telephone line is in his name, the Secret Service came and confiscated his equipment Its not right that this happened because of third party theft of service.

BG: I think the rationale is over simplistic.

B: Am I responsible for what you say when I answer my phone is essentially the question.

BG: No, I think the question is, is the bulletin board operator responsible for what is posted on his bulletin board.

B: Well that literally makes no sense. If a telemarketer calls me am I responsible for anything he says after I pick up the phone?

BG: A bulletin board is used to disseminate information further. When a person posts something, in this case a code, the bulletin board is used to further spread that information.

JM: I believe that is the Tom Tcimpidis case that you're referring to and I'm quite familiar with it. It was not quite as you put it. The stolen AT&T calling card that was posted was posted anonymously one minute and one minute after the AT&T card being posted by the anonymous party, Tom Tcimpidis, the sysop, the operator of the bulletin board himself had been on-line and had posted other messages. So there was reason to believe perhaps that the anonymous person was actually the system operator. There was a further complication that arose in that the stolen AT&T card belonged to a former employer of the system operator. Ultimately there was not enough evidence with which to charge anybody and the whole thing was quietly dropped, but it did raise some interesting questions as to responsibilities of the system operator because Mr. Tcimpidis said that he didn't know the code was there and yet his own equipment log showed that he had been on-line.

B: Let's take that a little further then. Let's say there was an answering machine connected to his phone and we know he listened to the answering machine. Let's say somebody with a voice message left him half a dozen stolen credit card numbers. Would the action of the law enforcement agencies have been the same?

JM: No...no, you're

B: I think you must look at a situation where over the years an unnecessary fear has grown of some of the hackers. The phone phreaks scare me to an extent. I've got bogus calls on my US. Sprint and All-Net bills, never got one on my AT&T bill. I can see this is a definite problem, the phone phreaks do scare me, and I realize that real problem is that nobody seems to reconcile every call or even read their long distance bills.

AA: If I have an answering machine on my phone and somebody calls up and leaves me information that were I to use it it would be illegal and I either erase the information or turn that other person in. I have no intent to use it and there is no law enforcement officer that I can imagine who is going to take action and no prosecutor who would take the case.

ES: In other words if a guy sets up a computer bulletin board for the express purpose of exchanging information he is not supposed to have when other people have information their not supposed to have, I don't think there's any doubt about what their intent is and about the fact that they are violating the law.

Sarge, if you went after somebody like Anna for what she admitted doing, stealing $15,000 dollars worth of long distance and you were able to handle the investigation, come up with the evidence, and bust her, what kind of penalty might she get?

AA: A very difficult question to answer because it depends upon her prior criminal history. Most of these hackers do not have a history. In Anna's case the crime would be a class four felony which would result in probably simple felony probation.

ES: She admitted to stealing $15,000!

AA: I'm sure that her estimate is wildly off on the low end. if she is disseminating codes then she is also somewhat responsible for other people's use of the same codes.

ES: Could we charge someone like her with conspiracy?

AA: Sure!

ES: She is generating a continuing criminal enterprise.

AA: It depends again on whether you choose to prosecute her federally or at the state level. She would be looking here at a class three or class two felony depending upon the sum of money that she had stolen.

ES: The bottom line here is if the punishment doesn't fit the crime, its not going to stop the criminals.

AA: You have to remember that these are the people who have not been processed in the criminal justice systems and even to hold them over the weekend in Cook County would not be an experience I'd care to repeat.

ES: Many of them are pretty arrogant sounding it seems.

(Commercial Break And Reintroductions)

ES: We’ve got an interesting new telephone law here; Chapter 38 of the Illinois Criminal Code. A person can be prosecuted, arrested and convicted for bothering somebody even if the person doesn’t answer the phone. Just ringing a persons phone now is against the law, it’s harassing them.

JM: I might add, since we’re discussing harassment by phone... the hackers don’t like me too well and I’ll get about a death threat a week from a hacker.

ES: Really.

JM: Oh yeah and every now and then I figure out who it was and I call them back and that kind of shakes up a little bit.

ES: There was this reporter here that was being harassed like crazy in the news department here by a hacker who had a computer that was ringing the phone. He was ringing the phones like crazy and I didn’t know about. Finally the reporter asked what I could recommend. I made a phone call and the Illinois Bell Security did what it had to do and then the Chicago Police were brought in and one night when I was on the air the officers went to guys home, knocked on the door, and this kid was shocked! He was a telemarketing representative for a major magazine and apparently he was working at home he had some of their equipment at home including a rapid dialer. He’s got two detectives at the front door and he had literally just gotten off the phone. We’ve got all the data and so now comes the decision what do you want to do. Take him to court? Lock him up? Go to his boss? I went back to the reporter in our news room and asked him what he wanted to do about it?

JM: What did he say?

ES: Write a 500 word essay on why he was never going to do it again.

JM: Ha Ha! We had one 14 year old one hacker who was on the bulletin boards and posting messages about how to make pipe bombs, different types of poison, long distance codes, and computer passwords, etc. On the bulletin boards he would come across like Ghengis Khan or or Joseph Stalin or something. I mean his language was all four letter words and yet face to face he was a very meek, mild mannered, well behaved youngster. However, get him behind the keyboard and he just sort of changes personality. What do you do to a 14 year old? He is much too young to really be put through any of the the serious criminal prosecutions so his penalty was that he had to read out loud to his parents all of the messages that he’d posted on the bulletin boards, four letters words and all. And that cured him... hahaha.

In most of the cases I’ve worked on it’s rare that someone goes to jail. I think the longest sentence that I’ve been involved with was probably like 30 days. I think there was one fellow down in Virginia, if I recall correctly, that got 90 days. You don’t necessarily want to put these folks in jail because then they’ll meet the real crooks and teach them all these nifty tricks.

ES: God help us. Lets grab a call real quick here from Gordon. Hello Gordon, where are you calling from?

G: Hello, I’m calling from DeKalb, Illinois.

ES: You have a question for our panel...go ahead.

G: Yeah I do. I’m a graduate student in Criminology up here at Northern Illinois University and I’m kinda involved in some field research with the types of people that you’re discussing tonight. I’ve heard a lot of terms flying back and forth between phreakers and hackers and things like that. I’d like to hear some input from the people on the panel as far as how they define these types of activities, if they draw and distinctions between the two, and secondly, if anybody can add any insight into maybe just how many people are currently active in this type of activity.

JM: I could take that because one of my specialties is identification and gathering data about how many perpetrators there are. To answer the first question, a computer hacker would be someone who concentrates mainly on breaking into computer systems. The phone phreak would be someone who, like Anna we heard earlier tonight, just makes long distance calls for free. The problem is you can’t really separate them. The hacker needs to know the phone phreak tricks in order to break into computers in other states or other countries. Certainly the phone phreak perhaps needs some computer aids in obtaining stolen codes. It is hard to separate them. You can call them phreakers or you can call them hackers or you can just call them criminals.

As to how many, this is a tough one because at what point to you draw the line? Do you say somebody that makes fifteen thousand dollars worth of calls in a year is a phone phreak and somebody that makes $14,900 is not? The problem is that its been a tradition to rip off the phone company ever since day one. There has been phone phreaks for twenty-five or thirty years at least. Ever since we've had long distance dialing.

BG: The phone companies not the only one under siege either.

JM: There are thousands of hackers, I would say just in the state of Illinois there are several thousand active computer hackers.

G: Those hackers are the active ones? Would you say that most of them are involved in communicating via the bulletin board systems and voice mail-boxes and things like that or is this pretty much a solitary activity.

JM: There are a few solitary hackers, in fact the beginnings of hacking, 25-30 years ago, it was a solitary activity. The bulletin boards have changed all that. Now the hackers no longer really operate in solitude.

AA: One thing also about the criminal element here, the hacker and the phreakers, my experience has been that we have had very few "clean" if you will, computer frauds. We have had some people who are only into multi-level marketing of codes, which ends up being enormous sums of money, but very often we've found that hackers are involved in other things too. For example, credit card frauds, we have done search warrants and found a reasonable quantities of illegal substances, of weapons, of other evidence of other offenses. We have probably easily 50% of our warrants turn up other things besides computer fraud. Which I think is an interesting point to keep in mind.

ES: Very good point.

(Break For Commercial and re-introductions)

R: Hello, I just wanted to call up and clarify something concerning computer hackers. I'm a hacker, but I'm not a criminal.

ES: We'll be the judge of that Bobby.

R: I think you will be. The reason I say that is, you're confusing things. The hacker is term that you could apply or compare more or less to "ham." It's a computer hobbyist, whether he does it just on his machine at home or he accesses legitimate services throughout the country and pays for his services he's a hacker. There are a lot of people who are irresponsible, mostly teenagers, who are quite impressed with the power of this machine and get carried away with it and do criminal acts. They happen to be hackers, but they're also criminals. I think that distinction.

CM: I think the point is well taken I think originally the hacker was a very positive term historically and for whatever reasons the word hacker has taken on some negative connotations.

R: Yes and that is unfair because I know legions of people who are hackers.

JM: I consider myself to be a hacker, but I'm certainly not a computer criminal (No, at least not a COMPUTER criminal). I mean my business is catching the criminal hackers. If we go back to 1983 when hackers made headlines for the first time, that was the Milwaukee 414 gang, they called themselves hackers and so right away the good term, hacker being someone who could do wonderful things with a computer got turned into someone who could do criminal things with a computer.

ES: I remember back to a time a few years ago when there was a group of criminals that got busted for coming up with a device called a black box which they used to circumvent paying the tolls you know on long distance phone charges. Was that kind of the beginning of this computer misbehavior? I mean was that a computer device?

JM: There are several boxes; the black box, blue box, red box, silver box, etc. I must confess that back when I was a teenager, over thirty years ago, there were not any computers to play around with, but there was this wonderful telephone network called the Bell System. I was one of the original inventors of the device known as the black box and another device known as the blue box (Yeah right, YOU invented these). In those days the phone network was such that you could manipulate it with very simple tone signals.

A black box essentially allows all calls to your phone to be received free of charge to the caller. In other words if somebody called you from a payphone they got their dimes back and if someone dialed you direct long distance they never got a bill.

The blue box was a little more insidious. It allows you to actually take over the long distance lines and dial direct anywhere in the world. I got into it just out of curiosity as a true hacker and I found out that these things were possible and I told a friend of mine at the phone company about what I could do with their circuits and of course he turned me into the security people.

It never really got started, but I do have sitting here in front of me a device that makes some of those tones. You could call it a blue box. I guess this is legitimate piece of test equipment, but let’s see if it will pick up. (Beeeep!)

ES: Came through loud and clear.

JM: The blue box today is obsolete, it really doesn’t work anymore. There, there are a few circuits that still us those kind of signals, but back 25-30 years ago that was the way to make your free phone calls. You didn’t have Sprint and MCI to abuse.

S: I’m a consulting engineer now but, I have been a communications manager for three Fortune 500 companies. One of the reasons I was hired was to put a stop to some long distance calling that had cost that company over a million and a half dollars in 27 months. We found the person that was doing it and he got a suspended sentence of six months. Then we turned around and sued him in civil court.

ES: We’ve got to start treating these criminals like criminals. Suspended sentences are unacceptable, hard jail time is absolutely mandatory and unfortunately, and I think that sergeant you probably will agree with me, it must be very frustrating to spend all the hours you do chasing people and even when you get them to plead guilty seeing how easy sometimes they get away.

AA: Oh sure.

S: How many people do you have assigned to your unit here in this state sarge?

AA: You’re talking to 50% of the unit.

(Break for commercials and re-introductions)

ES: Okay Ray, go ahead.

R: You would not believe how long I’ve been trying to get in touch with you. Since I was 14 years old, every time I’ve called, you’ve been busy.

ES: So how old are you tonight?

R: 18

ES: Four years!? What’s on your mind?

R: I used to pirate games when I was younger. As a matter of fact when I was 14. I mean my Dad had just bought me a computer and modem and I was pumped. People are always complaining about it, but it’s so easy for a 14 year old kid to do this, don’t you think that they should make it a little bit harder? Do you understand what I’m trying to say?

ES: Yes, but Ray it’s easy to steal a car. If your neighbor leaves his car in the driveway with the key in the ignition does that give you the right to take it?

R: I know I did wrong, but there is no way I can give it back. Its just stupid because when you get older you feel guilty about things.

ES: What did you used to do?

R: I used to call up certain places and I would like break in and take their games and then just keep them for myself.

BG: It was more entertainment for you?

R: It kept me occupied and it was so easy that I began to think that maybe it was meant to be easy so they could get publicity.

JM: There is perhaps a difference because when you copy a a computer program you can’t tell it from an original, but if you make a copy of a tape or a record it doesn’t sound quite the same.

CM: When you’re 14 years old it’s something new, right?

R: I got the biggest pump out of it.

CM: I think you did something for your ego and it gave you a sense of power.

ES: Okay Ray

R: Bye

ES: I’ve really enjoyed this program, but we’re out of time. John, I want to thank you for staying up and I have a feeling that we’ll do more radio because you’re an interesting guy.

JM: Thank you. It’s been interesting talking with you. By the way, I think I

know who Anna is, but we’ll keep that a secret from our listeners.
ES: Oh. Well why don’t you just tell the FBI?
JM: The Secret Service, yes.
ES: Right and I want to thank everyone else for being on the show tonight.
Everyone: Its been our pleasure. Lets do it again some time.