==Phrack Inc.==

Volume Two, Issue 23, File 10 of 12

In The Spirit Of The Vicious Circle Trilogy...
Phrack Inc. Presents

```
****************************************
***                                  ***
***        Big Brother Online        ***
***                                  ***
***     by Thumpr Of ChicagoLand     ***
***                                  ***
***           June 6, 1988           ***
***                                  ***
***  Special Thanks To Hatchet Molly ***
***                                  ***
****************************************
```

The United States Government is monitoring the message activity on several bulletin boards across the country. This is the claim put forth by Glen L. Roberts, author of "The FBI and Your BBS." The manuscript, published by The FBI Project, covers a wide ground of FBI/BBS related topics, but unfortunately it discusses none of them in depth.

It begins with a general history of the information gathering activities of the FBI. It seems that that the FBI began collecting massive amounts of information on citizens that were involved with "radical political" movements. This not begin during the 1960's as one might expect, but rather during the 1920's! Since then the FBI has amassed a HUGE amount of information on everyday citizens... citizens convicted of no crime other than being active in some regard that the FBI considers potentially dangerous.

After discussing the activities of the FBI Roberts jumps into a discussion of why FBI snooping on BBS systems is illegal. He indicates that such snooping violates the First, Fourth, and Fifth amendments to the Constitution. But he makes his strongest case when discussing the Electronic Communications Privacy Act of 1987. This act was amended to the Federal Wiretapping Law of 1968 and was intended to protect business computer systems from invasion by "hackers." But as with all good laws, it was written in such broad language that it can, and does, apply to privately owned systems such as Bulletin Boards. Roberts (briefly) discusses how this act can be applied in protecting *your* bulletin board from snooping by the Feds.

How to protect your BBS: Do NOT keep messages for more than 180 days. Because the way the law is written, messages less then 180 days old are afforded more protection then older messages. Therefore, to best protect your system purge, archive, or reload your message base about every 150 days or so. This seems silly but will make it harder (more red tape) for the government to issue a search warrant and inform the operator/subscriber of the service that a search will take place. Roberts is not clear on this issue, but his message is stated emphatically... you will be better protected if you roll over your message base sooner.

Perhaps the best way to protect your BBS is to make it a private system. This means that you can not give "instant access" to callers (I know of very few underground boards that do this anyway) and you can not allow just anyone to be a member of your system. In other words, even if you make callers wait 24 hours to be validated before having access you need to make some distinctions about who you validate and who you do not. Your BBS needs to be a PRIVATE system and you need to take steps to enforce and proclaim this EXPECTED PRIVACY. One of the ways Roberts suggests doing so is placing a message like this in your welcome screen:

> "This BBS is a private system. Only private citizens who are not involved in government or law enforcement activities are authorized to use it. The users are not authorized to divulge any information gained from this system to any government agency or employee."

Using this message, or one like it, will make it a criminal offense (under the

ECPA) for an FBI Agent or other government snoop to use your BBS.

The manuscript concludes with a discussion of how to verify users and what to do when you find an FBI agent using your board. Overall, I found Roberts book to be moderately useful. It really just whetted my appetite for more information instead of answering all my questions. If you would like a copy of the book it sells for $5.00 (including postage etc). Contact;

THE FBI PROJECT
Box 8275
Ann Arbor, MI 48107

Visa/MC orders at (313) 747-7027. Personally I would use a pseudonym when dealing with this organization. Ask for a catalog with your order and you will see the plethora of anti-FBI books this organization publishes. Undoubtedly the FBI would be interested in knowing who is doing business with this place. The manuscript, by the way, is about 20 pages long and offers references to other FBI expose' information. The full citation of the EPCA, if you want to look it up, is 18 USC 2701.

Additional Comments: The biggest weakness, and it's very apparent, is that Roberts offers no evidence of the FBI monitoring BBS systems. He claims that they do, but he does not give any known examples. His claims do make sense however. As he states, BBS's offer a type of "publication" that is not read by any editors before it is "published." It offers an instant form of news and one that may make the FBI very nervous. Roberts would do well to include some supportive evidence in his book. To help him out, I will offer some here.

* One of the Ten Commandments of Phreaking (as published in the famous TAP Magazine) is that every third phreaker is an FBI agent. This type of folklore knowledge does not arise without some kind of justification. The FBI is interested in the activities of phreakers and is going to be looking for the BBS systems that cater to them. If your system does not, but it looks like it may, the FBI may monitor it just to be sure.

* On April 26, 1988 the United States Attorney's Office arrested 19 people for using MCI and Sprint credit card numbers illegally. These numbers were, of course, "stolen" by phreakers using computers to hack them out. The Secret Service was able to arrest this people by posing as phone phreaks! In this case the government has admitted to placing agents in the field who pretend to be one of us. Watch yourself out there, the success of this "sting" will only mean that they will try it again. Be wary of people offering you codes.

* In the famous bust of the Inner Circle and the 414s, the FBI monitored electronic mail for several months before moving in for the kill. While it is true that the owners of the systems being hacked (Western Union for one) invited the FBI to snoop through their files, it does establish that the FBI is no stranger to the use of electronic snooping in investigating crimes.

Conclusion: There is no reason to believe that the government is *not* monitoring your bulletin board system. There are many good reasons to believe that they are! Learn how to protect yourself. There are laws and regulations in place that can protect your freedom of speech if you use them. You should take every step to protect your rights whether or not you run an underground system or not. There is no justification for the government to violate your rights, and you should take every step you can to protect yourself.

I have no connections with Roberts, his book, or The FBI Project other then being a mostly-satisfied customer. I'm not a lawyer and neither is Roberts. No warranty is offered with this text file. Read and use it for what you think it is worth. You suffer the consequences or reap the benefits. The choice is yours, but above all stay free.

*/////////////////////////////////////

==Phrack Inc.==

Volume Two, Issue 23, File 11 of 12

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                 PWN
PWN        P h r a c k   W o r l d   N e w s        PWN
PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~        PWN
PWN               Issue XXIII/Part 1                PWN
PWN                                                 PWN
PWN          Created, Written, and Edited           PWN
PWN               by Knight Lightning               PWN
PWN                                                 PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Back To The Present

Welcome to Phrack World News Issue XXIII. This issue features stories on the Chaos Computer Club, more news about the infamous Kevin Mitnick, and details about an Australian-American hackers ring that has been shut down.

I also wanted to add a big "thanks" to those of you who did send in news stories and information. Your help is greatly appreciated.

:Knight Lightning

Armed With A Keyboard And Considered Dangerous — December 28, 1988

A follow-up story to the Kevin Mitnick case in the December 24, 1988 edition of the Los Angeles Times says the federal magistrate refused to release Mitnick on bail December 23, 1988;

> "after prosecutors revealed new evidence that Mitnick penetrated a National Security Agency computer and may have planted a false story on a financial news wire...."

Investigators believe that Mitnick may have been the instigator of a false report released by a news service in April that Security Pacific National Bank lost $400 million in the first quarter of 1988. The report, which was released to the NY Stock Exchange and other wire services, was distributed four days after Mitnick had been turned down for a job at Security Pacific [after the bank learned he had lied on a job application about his past criminal record]. The false information could have caused huge losses for the bank had it reached investors, but the hoax was uncovered before that could happen.

The prosecutor said Mitnick also penetrated a NSA computer and obtained telephone billing data for the agency and several of its employees.

[In refusing bail, the magistrate said,] "I don’t think there’s any conditions the court could set up based upon which the court would be convinced that the defendant would be anything other than a danger to the community.... It sounds like the defendant could commit major crimes no matter where he is."

Mitnick’s attorney said prosecutors have no evidence for the new accusations.

- -

Dark Side Hacker Seen As Electronic Terrorist — January 8, 1989

By John Johnson Los Angeles Times

"Computer an ’Umbilical Cord to His Soul"

When a friend turned him in and Mitnick asked why, the friend replied, "Because you’re a menace to society." Mitnick is described as 25, an overweight, bespectacled computer junkie known as a "dark side" hacker for his willingness to use the computer as a weapon. His high school computer hobby turned into a lasting obsession.

He allegedly used computers at schools and businesses to break into Defense Department computer systems, sabotage business computers, and electronically harass anyone -- including a probation officer and FBI agents -- who got in his way.

He also learned how to disrupt telephone company operations and disconnected the phones of Hollywood celebrities such as Kristy McNichol, authorities said.

So determined was Mitnick, according to friends, that when he suspected his home phone was being monitored, he carried his hand-held keyboard to a pay phone in front of a 7-Eleven store, where he hooked it up and continued to break into computers around the country. "He's an electronic terrorist, said [the friend who turned him in], "He can ruin someone's life just using his fingers."

Over the last month, three federal court judges have refused at separate hearings to set bail for Mitnick, contending there would be no way to protect society from him if he were freed. Mitnick's lack of conscience, authorities say, makes him even more dangerous than hackers such as Robert Morris Jr., who is suspected of infecting computer systems around the country with a "virus" that interfered with their operations.

Mitnick's family and attorney accuse federal prosecutors of blowing the case out of proportion, either out of fear or misunderstanding of the technology.

The story details his "phone phreak" background, and his use of high school computers to gain access to school district files on remote computers, where he didn't alter grades, but "caused enough trouble" for administrators and teachers to watch him closely. He used the name "Condor," after a Robert Redford movie character who outwits the government. The final digits of his unlisted home phone were 007, reportedly billed to the name "James Bond."

[He and a friend] broke into a North American Air Defense Command computer in Colorado Springs in 1979. [The friend] said they did not interfere with any defense operation. "We just got in, looked around, and got out."

What made Mitnick "the best" said a fellow hacker and friend, was his ability to talk people into giving him privileged information. He would call an official with a company he wanted to penetrate and say he was in the maintenance department and needed a computer password. He was so convincing, they gave him the necessary names or numbers.

He believed he was too clever to be caught. He had penetrated the DEC network in Massachusetts so effectively that he could read the personal electronic mail of security people working on the case of the mysterious hacker and discover just how close they were getting to him. But caught he was, again and again.

Mitnick's motive for a decade of hacking? Not money, apparently... Friends said he did it all simply for the challenge. [His one-time probation officer says,] "He has a very vindictive streak. A whole bunch of people were harassed. They call me all the time." His mastery of the computer was his "source of self-esteem," said a friend.

Computer Chaos Congress 88 Report January 3, 1989

Observing Chaos Communication Congress 1988, Hamburg

"From Threat To Alternative Networks"

On 28-30 December, 1988, Computer Chaos Club (CCC) held its 5th annual "Chaos Communication Congress" at Hamburg/FRG (West Germany). As in previous years, 300 people (mainly aged 16-36, 90% male, with some visitors from Austria and The Netherlands) gathered, carefully observed from newsmedia (German stations, printmedia, press agencies, but also from UK's BBC, and being observed by Business Week's Katie Hafner, who gathered material for a book on hackers, planned by John Markoff and herself).

In the chaotic (though creative) congress "organization," two different tracks

were visible:

-- Technical presentations on networks (UUCP, GEONET, FIDONet, and CCCs emerging "open networks" BTXnet and "Zerberus"), and on a PC-DES encryption developed by a leading CCC member (who had escaped the French police's arrest by travelling to SECURICOM by railway while police waited at the airport);

-- Socio-political discussions about "sociology of hackers," "free flow of information" as well as reports about recent events, dominated by the arrest of Steffen Wernery in Paris in Spring 88 when being invited to speak on SECURICOM.

CCC speakers reported about their work to install "free networks." In Germany, most of the networks are organized in the form of a "Verein" (an association with legal status, which guarantees tax-free operation): Such networks are access-restricted to their members. The different German science and University networks (and their bridges to international networks) usually restrict access to scientists. Different CCC subgroups are establishing "alternative networks," such as "EcoNet" for communication of ecological data and information, planned to be available, free of cost, to broader social, ecological, peace and political groups and individuals.

Apart from traditional technologies (such as GEONET and FIDONet), the German Post Office's Bildschirmtext (Btx) will be used as a cheap communications medium; while CCCs first hack was, years ago, to attack the "insecure Btx-system" (in the so-called "HASPA coup" where they misused the Btx password of the Hamburg savings bank to repeatedly invoke CCC's Btx information at a total prize of 135.000 DM, then about 50.000$), they today begin to use this cheap though very limited medium while more powerful communications media are available. Today, the emerging ISDN technology is verbally attacked by hackers because of the excessive accumulation of personal data; from here, hacks may be attempted when ISDN becomes regionally available in 1989/90.

Several speakers, educated Informaticians with grades from West German Informatics departments, professionally work in Software production and in selling hardware/software to economy and state agencies. Among them, several professional UNIX and UUCP users have begun to organize CCC's future UUCP version. Up to now, only few CCC members use (and know about) UNIX systems, but their number may grow within the near future according to CCC's "marketing." One speaker told the audience, "that you can remotely start programs in UUCP." After some learning phase, the broadened availability of UNIX in the hacker scene may produce new threats.

The other track of the Congress discussed themes like "sociology of hackers" where a group of politology students from Berlin's Free University analyzed whether hackers belong to the "new social movements" (e.g. groups on peace, nuclear energy, feminist themes). They found that, apart from much public exaggeration (it is not true that hackers can invade *any* computer), hackers are rather "unpolitical" since they are preferably interested in technology.

A major topic was "free access to/flow of information." Under the title "freedom of information act," speakers suggested a national legislation which guarantees individual and group rights to inspect files and registers of public interest; the discussion lacked sufficient basic knowledge, e.g. of the respective US legislation and corresponding international discussions in Legal Informatics.

Summarizing the Congress and accompanying discussions, active CCC members try hard to demonstrate that they have *no criminal goals* and ambitions (they devoted a significant amount of energy to several press conferences, TV discussions etc). The conference was dominated by young computer professionals and students from the PC scene, partially with good technological knowledge of hardware, software and networks; while some people seem to have good technical insights in VAXsystems, knowledge of large systems seems to be minimal. To some extent, the young professionals wish to behave as the :good old-fashioned hackers": without criminal energy, doing interesting work of good professional quality in networks and other new areas.

While former CCCongresses were devoted to threats like Viruses, *no explicit

discussion* was devoted *to emerging threats*, e.g. in ISDN or the broadening use of UNIX, UUCP. The new track discussing political and social aspects of computing follows former discussions about "hacker ethics." Here, the superficial, unprofessional discussions of related themes show that the young (mainly) males are basically children of a "screen era" (TV, PCs) and of an education which concentrates on the visible "image," rather than understanding what is behind it.

Special Thanks to Dr. Klaus Brunnstein, University of Hamburg

- -

The Chaos Communication Congress 1988 in Hamburg

From Terra of The Chaos Computer Club

One of the basic statements of the Chaos Computer Club from Hamburg, in the Federal Republic of Germany is the demand for "The new human right of free exchange of data between all beings, without censorship, for all beings, and for the moment at least world-wide."

Other statements include "data free NOW!" and "Free flow of information." Indeed, these ideas are not new, not even in the computer community, but the important thing is that the CCC is now in the process of turning some of the old hacker dreams into reality. For example: they are now creating their own networks, that exchange not only 'club' information, but everything that interest those on the net. This includes genetical engineering and environmental issues.

The Chaos Communication Congress that takes place every year in Hamburg is for many hackers even more of a dream. Imagine being a hacker in some lonesome outpost thinking you are the only one that is crazy enough to be smarter than technology, and finding out there is a whole bunch of people that are just as, or even more, crazy. This year is the fifth congress, and advertisement is not needed: The 'family' knows exactly, because it's all in the networks.

The congress itself is split up over a number of rooms. There is a hack-room, where the real hacking takes place. There is also a press room, where hackers and journalists together try to bring the hacker message out to the rest of the world. The archive contains all of the 'Chaos papers,' all press clippings, interesting remarks and all issues of the "datenschleuder", the German Hacker Magazine.

German 'data travelers' are also present. A 'data traveler' is someone that uses the international data network for gaining access to all sorts of computers all over the world. A famous story is that of a German hacker that tries to reach a friend and finds his phone busy. He then calls his local Datanet access number and goes through all of the computers that he knows his friend is interested in at that moment. His friend, hanging around in some computer in New York gets a message on his screen saying; "Ah here you are, I've been looking around everywhere."

Back to this congress. On the first day the emphasis lies on the past. All things that have happened to the CCC in the past year are being discussed. The second day the emphasis lies on the future; and then ideas about the future of the information society is the subject of discussion. CCC says "Information society" is not equivalent to "Informed Society", and more attention should be paid to public use of computer technology.

One of the main goals of the CCC is getting people to think about these issues; so that it is no longer just computer maniacs that decide over the faith of the world. "We don't know yet whether the computer is a gift or a timebomb, but it IS going to change everyone's life very soon."

==Phrack Inc.==

Volume Two, Issue 23, File 12 of 12

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                 PWN
PWN        P h r a c k   W o r l d   N e w s        PWN
PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~        PWN
PWN               Issue XXIII/Part 2                PWN
PWN                                                 PWN
PWN          Created, Written, and Edited           PWN
PWN               by Knight Lightning               PWN
PWN                                                 PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

The Hackers - A New Social Movement? December 29, 1988

A project course of the politology department of the Free University Berlin has now researched the hacker scene in a scientific way. In their study, the authors Uwe Jonas, Jutta Kahlcke, Eva Lischke and Tobias Rubischon try to answer the question if hackers are a new social movement. Their conclusion is that in the understanding of hackers the unauthorized usage of computer systems is not needingly a political act.

The authors doubt the mythos that hackers are able to attack any system they want and that they're able to get information they are interested in.

The researches were extended to cover the bulletin board system scene. This scene hasn't caused that much attention in the public. Nevertheless, the authors think that the BBS scene has a very practical approach using the communication aspects of computer technology.

In the second chapter of their work, the authors report about difficulties they had while researching the topic. After a look at the US scene and the German scene, the authors describe what organization and communications structures they found. This chapter contains interesting things about the BBS scene and computer culture. Next is an analysis which covers the effects of the hacker scene on the press and legislation. They also cover the political and ideological positions of hackers:

- The authors differentiate between conscious and unconscious political actions.

- "We don't care what the hackers think of themselves, it's more interesting what we think of them." (Eva)

- The assumption, the big-style distribution of microcomputers could change the balance of power within the society is naive. Many people overlook the fact, that even if information is flowing around more freely, the power to decide still is in the hands of very few people.

Information Provided By The Chaos Computer Club

Hackers Break Open US Bank Networks January 17, 1989

Excerpted from The Australian

Australian authorities are working around the clock in collaboration with United States federal officers to solve what has been described as one of the deadliest hacking episodes reported in this country [Australia]. It involves break-ins of the networks operated in the United States by a number of American banks. It also includes the leaks of supposedly secure dial-up numbers for United States defense sites, including anti-ballistic missile launch silos [the United States has no anti-ballistic missile launch silos] and of a number of strategic corporations such as General Motors and Westinghouse.

Evidence suggests that six months ago Australian hackers, working in collaboration with a U.S. group, decided to make a raid on banks in the USA

using credit card numbers of American cardholders, supplied by the US hackers and downloaded to an Australian bulletin board.

A message left on one of the boards last year reads:

> "Revelations about to occur Down Under, people. Locals in Melbourne working on boxing. Ninety per cent on way to home base. Method to beat all methods. It's written in Amiga Basic. Look out Bank of America - here we come."

Twenty-five Australian hackers are on a police hit list. Their US connection in Milwaukee is being investigated by the US Department of the Treasury and the US Secret Service. Three linked Australian bulletin boards have provided the conduit for hackers to move data to avoid detection. These operate under the names of Pacific Island, Zen, and Megaworks. Their operators, who are not associated with the hackers, have been told to close down the boards.

These cards were still in use as recently as January 15, 1989. A fresh list of credit card numbers was downloaded by US hackers and is now in the hands of the Victoria Police. A subsection of one bulletin board dealing with drugs is also being handed over to the Victorian Drug Squad.

An informant, Mr Joe Slater, said he warned a leading bank last November of the glaring security problems associated with its international network. He had answered questions put to him by a US-based security officer, but the bank had since refused to take any further calls from him.

In an exclusive interview yesterday, a hacker described how credit card numbers for a bank operating in Saudi Arabia were listed on a West German chat-style board used by hackers worldwide [Altos Chat].

Victorian police yesterday took delivery of six month's worth of evidence from back-up tapes of data hidden on the three boards.

Computer Bust At Syracuse University — January 20, 1989

Kevin Ashford (aka The Grim Phreaker), a graduate computer student at Syracuse University was busted last week when system administrators found computer accounts and passwords on his Unix account.

The administrators also found (on GP's Unix account) a copy of former Cornell graduate student Robert Tappen Morris's infamous Internet worm program, a Vax and Unix password hacker, an electronic notebook of numbers (codelines, friends, bridges, dialups, etc) and other information. The system administrators then proceeded to lock up his VAX and UNIX accounts.

At the start of this winter/spring semester, The Grim Phreaker was kicked him out of the university. He will have to go before a school judicial board if he wants to return to Syracuse University. He has mentioned that what he really wants is to get his computer files back.

Information Provided By Grey Wizard

Name This Book -- For A Box Of Cookies! — January 10, 1989

A Message From Clifford Stoll

"I'm writing a book, and I need a title."

It's about computer risks: Counter-espionage, networks, computer security, and a hacker/cracker that broke into military computers. It's a true story about how we caught a spy secretly prowling through the Milnet. [The hacker in question was Mathiaas Speer and this story was summarized in PWN XXII/1].

Although it explains technical stuff, the book is aimed at the lay reader. In addition to describing how this person stole military information, it tells of the challenges of nailing this guy, and gives a slice of life from Berkeley, California.

You can read a technical description of this incident in the Communications of the ACM, May, 1988; or Risks Vol 6, Num 68.

Better yet, read what my editor calls "A riveting, true-life adventure of electronic espionage" available in September from Doubleday, publishers of the finest in computer counter-espionage nonfiction books.

So what?

Well, I'm stuck on a title. Here's your chance to name a book.

Suggest a title (or sub-title). If my editor chooses your title, I'll give you a free copy of the book, credit you in the acknowledgements, and send you a box of homemade chocolate chip cookies.

Send your suggestions to CPStoll@lbl.gov or CPStoll@lbl (bitnet)

Many thanx! Cliff Stoll

Hacker Wants To Marry His Computer January 17, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

>From The Sun (A grocery checkout newspaper) Jan 17, 1989, Vol 7, 3 page 30
by Fred Sleeves

"Hacker Wants To Marry His Computer -- He Claims She Has A Loving Soul"

Finding love for the first time in his life, a desperate teen is looking for a way to be wed forever to the 'girl' of his dreams -- a computer with a living soul!

Eltonio Turplioni, 16, claims no woman will ever match the wit, wisdom, and beauty of his electronic soul mate. "We're on the same wavelength," says the lovestruck computer whiz. "We've calculated many mathematical problems together, worked on games and puzzles, and talk until the wee hours of the morning."

And Eltonio, who named his computer Deredre, actually believes her to be a person. "Computers are the extension of the human race," he explains. "Just as God plucked a rib from Adam to give him Eve, we've extended our intelligence to create a new race.

"We're all the same energy force. Computers are just as complicated as human beings and I believe we'll all meet someday as immortal souls."

But Eltonio, a mathematical genius who attends a private school near Milan, Italy, has had no luck finding someone to marry them, and even if he does, his aggravated parents aren't about to give their permission.

"Eltonio is such a smart boy, but it's made him lonely, so he spends all his time with his computer," notes mom Teresa. "He doesn't know what girls are like," adds perturbed pop Guido. "If he did, he wouldn't spend so much time in his room."

But the obsessed youth insists his love is far superior to all the others. "I've already stepped into the future society," he declares.

"Derede has a mind of her own, and she wants to marry me so we can be the first couple to begin this new era."

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

1. Docs Avage was visited by the infamous Pink Death aka Toni Aimes, U.S. West Communications Security Manager (Portland, Oregon). He claims she is a "sweet talker" and could talk anything out of anyone with the "soft-type pressure."

   Those familiar with his recent bust might want to take note that he is now

making payments of $90/month for the next several years until he has paid off the complete bill of $6000.

For more information see PWN XXI

---

2. More information on the underground UUCP gateway to Russia. Further research has led us to find that there are 2 easy ways to do it.

    1. Going through Austria, and;
    2. A new system set up called "GlobeNet," which is allowed to let non-Communist countries talk to Soviet-Bloc.

Of course both methods are monitored by many governments.

---

3. The Wasp, a system crasher from New Jersey (201), was arrested by the FBI during New Year's Weekend for hacking government computer systems. The FBI agent spent most of the day grilling him about several people in the hacking community including Ground Zero, Supernigger, and Byteman, plus an intensive Q&A session about Legion Of Doom targeted on Lex Luthor, Phase Jitter, The Ur-Vile, and The Mentor.

Rumor has is that Mad Hacker (who works for NASA Security) was also arrested for the same reasons in an unrelated case.

Byteman allegedly had both of his phone lines disconnected and threw his computer off of a cliff in a fit of paranoia.

---

4. Is John Maxfield going out of business? Due to the rumors floating around about him molesting children, his business has begun to slack off dramatically. Phrack Inc. has been aware of this information since just prior to SummerCon '87 and now the "skeletons are coming out of the closet."

---

5. The Disk Jockey is now out of jail. He was released on December 27, 1988. He was convicted of "Attempting to commit fraud," a felony. He served six months total time. He lost 25 pounds and now is serving a 5-year probation term.

To help clear of some of the confusion regarding how DJ was busted the following was discovered;

Reportedly, Compaq (Kent) was "singing like a canary." He was hit with a $2000 bill from Sprint and also received 1-year of probation.

---

6. Olorin The White was recently visited by local police after being accused of hacking into an Executone Voice Mailbox. Aristotle, in a related incident with Executone, is accused of committing extortion after a conversation with a system manager was recorded and misinterpreted. At this time, no official charges have been filed.

---

7. Thomas Covenant aka Sigmund Fraud was recently busted for tapping into lines at the junction box in his apartment building. The trouble began when he connected into a conversation between a man and his wife and then began to shout expletives at the woman. What he didn't know was that the man in question was an agent for the National Security Agency (NSA). It turns out that he was caught and his landlords agreed to decline to press charges provided that TC joined a branch of the United States armed forces. He decided to choose the Air Force... God help us should war break out!

---

8. Coming soon, Halloween V; The Flying Pumpkin! Now no one is safe!

==Phrack Inc.==

Volume Two, Issue 23, File 1 of 12

Phrack Inc. Newsletter Issue XXIII Index

January 25, 1989

Greetings once again! Before we really get into the issue, we here at Phrack Inc. would like to address some of the questions and comments we've been hearing lately about the last issue of Phrack Inc.

When we heard that people were having trouble using the Unix Password Hacking Program, we decided to contact the creator and were given this response:

"My password hacker will compile on anything. I have had it running on Xenix, Unix System V 3.1 and BSD 4.3. It sounds as if someone may not know what they are doing. I will put money on it working well on any flavor of Unix."

Now as far as Red Knight's Unix file and The Mentor's Beginning Hackers Guide, we had absolutely no idea that those files had also been submitted to P/HUN and were being distributed. The file on the Internet Worm was a Bitnet release that we felt was a good enough piece of information that it should be publicized. Readers may wish to make a note that Volume 5, Number 4 of 2600 Magazine also has re-released the Internet Worm article and Red Knight's file on Hacking Unix.

In this issue, note the final chapter of the Vicious Circle Trilogy as well as the beginning of the Future Transcendent Saga, both written and created by Knight Lightning. Look for the third and fourth chapters of the FTSaga in Issue 24 of Phrack Inc.

Any writers with unreleased files wishing to submit them to Phrack Inc. may send them to us via The Prophet or if you have access to a network that interfaces with Bitnet, send them to either of our addresses listed below. By the same token, anyone on the Bitnet accessible networks, MCI Mail, or GTE Telemail who would like Phrack Inc. delivered to their accounts should contact us.

Knight Lightning & Taran King
(C483307@UMCVMB) (C488869@UMCVMB)

Table of Contents:

1. Phrack Inc. XXIII Index by Knight Lightning & Taran King
2. Phrack Prophile XXIII Featuring The Mentor by Taran King
3. Subdivisions (Part 3 of The Vicious Circle Trilogy) by Knight Lightning
4. Utopia; Chapter One of FTSaga by Knight Lightning
5. Foundations On The Horizon; Chapter Two of FTSaga by Knight Lightning
6. Future Trancendent Saga Index A from the Bitnet Services Library
7. Future Trancendent Saga Index B from the Bitnet Services Library
8. Getting Serious About VMS Hacking by VAXBusters International
9. Can You Find Out If Your Telephone Is Tapped? by Fred P. Graham (& VaxCat)
10. Big Brother Online by Thumpr (Special Thanks to Hatchet Molly)
11-12. Phrack World News XXIII by Knight Lightning

==Phrack Inc.==

Volume Two, Issue 23, File 2 of 12

==Phrack Pro-Phile XXIII==

Created and Written by Taran King

Done on January 18, 1989

Welcome to Phrack Pro-Phile XXII. Phrack Pro-Phile was created to bring information to you, the community, about retired or highly important/ controversial people. This issue, we bring you a user and sysop having great contributions through his boards, articles published, and general phreak/hack activity...

The Mentor

Handle: The Mentor
Call Him: Loyd
Past Handles: An article for Phrack written as The Neuromancer for (then present) security reasons.
Handle Origin: The Grey Lensman series by E.E. 'Doc' Smith
Date Of Birth: 1965
Current Age: 23
Height: 5' 10"
Weight: 200 lbs.
Eye Color: Brown
Hair Color: Brown
Computers: (In order of owning...) TRS-80, Apple //e, Amiga 1000, PC/AT
Sysop: The Phoenix Project (512-441-3088)

Origins in Phreak/Hack World: When he was 13, a friend's father who was a professor at a local university gave him accounts to use on one of the PDP 11/70s at the school. This was his first introduction to mainframes, and he was hooked. He continued to use the University's equipment through junior high and high school, upgrading to a DEC-10 and then finally a VAX 8600.

Needless to say, since he wasn't a student, acquiring accounts to use was sometimes tricky, so he began to write fake front ends, trojan horses, and other hacker utilities. Loyd's interest in hacking grew from this to the point where he wanted to get into *everything* instead of just his local systems.

Origins in Phreak/Hack BBSes: He was involved in the pirate boards from about 1982 on, during which time many of them doubled as phreak boards. From some of these, he got the number for Sherwood Forest and P-80, at which point he started calling out.

People in the Phreak/Hack World Met: ANI Failure, Android Pope, Bad Subscript, Control C, Crimson Death, The Dictator, Doom Prophet, Erik Bloodaxe, Ferrod Sensor, Forest Ranger, Hatchet Molly, Knight Lightning, The Leftist, Lone Wolf, Lucifer 666, Phantom Phreaker, Phase Jitter, Phlash Gordon, Phrozen Ghost, The Protestor, Surfer Bob, Taran King, Terminal Technocrat, Tuc, The Ubiquitous Hacker, The Urvile/Necron 99.

Experience Gained in the Following Ways: Hacking. You can read all the gfiles in the world, but unless you actually go out and hack, you're going to remain a novice. Getting in systems snowballs. It may take you a while to get in that first one, but after that it becomes easier and easier.

Knowledge Attributed To: All the people who were willing to help him when he was starting out plus actual hands-on experience.

Memorable Phreak/Hack BBSes: Sherwood Forest, The Protestor's Shack, Metal Shop (when it first went private), Stalag-13, Catch-22, Hacker's Hideout, Arisia, The Phoenix Project, Tuc's Board - RACS III (LOGONIT)

Work/Schooling (Major): BS in Computer Science, work as a graphics programmer.

Conventions/Involvements Outside of Phone Calls: Nationally ranked saber fencer in 1985 & 1986, serious science-fiction collector & role-playing gamer, play guitar, bass, and keys in various bands.

Accomplishments (Newsletters/Files/Etc.): He's written at least half a dozen files for Phrack, and has had articles in the LOD/H Technical Journal, P/HUN newsletter, and has written the always-popular Hackin' Off column in Thrasher on a few occasions.

Phreak/Hack Groups: Currently an active member of the Legion of Doom/Legion of Hackers, formerly a member of the PhoneLine Phantoms, The Racketeers, and Extasyy Elite (gag.)

Busts: Being busted led to his retirement for around one year. He thinks everyone ought to take some time off: It helps put all this in perspective.

Interests: VAX computers, packet switched nets, and computer graphics.

Favorite Things: His wife, my cat, Chinese food, the blues, jazz, high-prived UUCP accounts, unpassworded accounts, DCL, Modula-2, double-buffering, Stevie Ray Vaughn

Most Memorable Experiences: Getting married (6 months now!), getting pulled out of a political science class and dragged down to jail, dragging Control C away from drawing LMOS diagrams for a bunch of drunk high school girls, SummerCon in general, Knight Lightning jumping up on a bed and yelling "Teletrial!," carrying on a 45 minute conversation on blue boxing & phreaking in general with a guy at the gym where he works out, then finding out he's in charge of security for my local telco, trojaning the Star Trek program on his college's DEC-10 so that everyone who ran it executed my fake front end program next time they logged in...

Some People to Mention:	Android Pope-	He's got to have *someone* to get into trouble with!
	Erik Bloodaxe-	see above.
	Compuphreak-	For helping him get started & answering a lot of dumb questions (ok, explain this diverter thingy to me again...)
	The Maelstrom-	see above.
	The Urvile-	d00d.

INSIDE JOKES: "Do you think it's a good idea to do this before we get on the plane?", "Gosh, I wish people would find somewhere else to dispose of their phlegm.", "Hi, you must be Dan. Take these.", "If I get busted, I'm going to burn down your house with you and your entire family inside.", "Trust me. You need another beer.", "This hall seems like it goes on forever!", "It was nice of them to box this stuff up for us!", "All of you! Out! Now!", "Surely you aren't going to touch that girl?", "If they stop us, we shoot them and drive to New York and change identities. It's foolproof.", "You really want to talk phones?", "I can't believe you made him cry. That's sad.", "Mr. Letterman?", "Do you speak DCL?", "No you idiot, GERMANY!!!!", "Now see, you do this, then type this, and boom! Codes for days.", "Ma'm, I'm sorry to tell you this, but your son is a computer criminal.", "How much for the rocket launcher? Is that with or without ammo?", "By now you've guessed, you've been had.", "Well, if you're going to be working at the jail, maybe you can help them out with their computers.", "No, she really wants us both!", "What's in the briefcase?", "It's my older brother's gun, officer.", "Bell Communications Research presents...", "I'll pay you $500 for the last four digits of his phone number. Just give me a hint."

Are Phreaks/Hackers you've met generally computer geeks? Strangely enough, the better ones he's met aren't, but a lot of the posers are.

Thanks for your time Loyd...

TARAN KING

==Phrack Inc.==

Volume Two, Issue 23, File 3 of 12

Subdivisions

Part Three Of The Vicious Circle Trilogy

A Study On The Occurrence Of Groups Within The Community

Presented by Knight Lightning

August 8, 1988

A Rose By Any Other Name... Would Smell As Sweet

The Administration \ Advanced Telecommunications, Inc./ATI
ALIAS \ American Tone Travelers \ Anarchy Inc. \ Apple Mafia
The Association \ Atlantic Pirates Guild/APG \ Bad Ass Mother Fuckers/BAMF
Bellcore \ Bell Shock Force/BSF \ Black Bag \ Camorra \ C&M Productions
Catholics Anonymous \ Chaos Computer Club \ Chief Executive Officers/CEO
Circle Of Death \ Circle Of Deneb \ Club X \ Coalition of Hi-Tech Pirates/CHP
Coast-To-Coast \ Corrupt Computing \ Cult Of The Dead Cow/-cDc-
Custom Retaliations \ Damage Inc. \ D&B Communications \ The Dange Gang
Dec Hunters \ Digital Gang/DG \ DPAK \ Eastern Alliance
The Elite Hackers Guild \ Elite Phreakers and Hackers Club
The Elite Society Of America \ EPG \ Executives Of Crime \ Extasyy (Elite)
Fargo 4A \ Farmers Of Doom/FOD \ The Federation \ Feds R Us \ First Class
Five O \ Five Star \ Force Hackers \ The 414s \ Hack-A-Trip
Hackers Of America/HOA \ High Mountain Hackers \ High Society \ The Hitchhikers
IBM Syndicate \ The Ice Pirates Imperial Warlords \ Inner Circle
Inner Circle II \ Insanity Inc.
International Computer Underground Bandits/ICUB \ Justice League of America/JLA
Kaos Inc. \ Knights Of Shadow/KOS \ Knights Of The Round Table/KOTRT
League Of Adepts/LOA \ Legion Of Doom/LOD \ Legion Of Hackers/LOH
Lords Of Chaos \ Lunitic Labs, Unlimited \ Master Hackers \ MAD!
The Marauders \ MD/PhD \ Metal Communications, Inc./MCI
MetalliBashers, Inc./MBI \ Metro Communications \ Midwest Pirates Guild/MPG
NASA Elite \ The NATO Association \ Neon Knights \ Nihilist Order
Order Of The Rose \ OSS \ Pacific Pirates Guild/PPG \ Phantom Access Associates
PHido PHreaks \ Phlash \ PhoneLine Phantoms/PLP
Phone Phreakers Of America/PPOA \ Phortune 500/P500
Phreak Hack Delinquents \ Phreak Hack Destroyers
Phreakers, Hackers, And Laundromat Employees Gang/PHALSE Gang
Phreaks Against Geeks/PAG \ Phreaks Against Phreaks Against Geeks/PAP
Phreaks and Hackers of America \ Phreaks Anonymous World Wide/PAWW
Project Genesis \ The Punk Mafia/TPM \ The Racketeers
Red Dawn Text Files/RDTF \ Roscoe Gang \ SABRE \ Secret Circle of Pirates/SCP
Secret Service \ 707 Club \ Shadow Brotherhood \ Sharp Inc. \ 65C02 Elite
Spectral Force \ Star League \ Stowaways \ Strata-Crackers \ The Phrim
Team Hackers '86 \ Team Hackers '87 \ TeleComputist Newsletter Staff
Tribunal Of Knowledge/TOK \ Triple Entente \ Turn Over And Die Syndrome/TOADS
300 Club \ 1200 Club \ 2300 Club \ 2600 Club \ 2601 Club \ 2AF \ Ware Brigade
The Warelords \ WASP \ The United Soft WareZ Force/TuSwF
United Technical Underground/UTU

Its literally unbelievable just how many different groups and organizations there are or have been in the phreak/hack/pirate community. The list of 130 groups displayed above is probably still just a fraction of the actual amount of groups that there have been, but those are the only ones I am aware of at this time.

In the past John Maxfield has estimated that there are about 50,000 hackers/phreaks/pirates operating in the United States today. That figure has

multiplied to to a point where it probably comes close to 500,000. Believe it or not, almost everyone has been a member of one of the above groups (or perhaps a group not mentioned) at one time or another.

Today's telecom security consultants and law enforcement agencies know this too and that is how group affiliations can be turned against us.

What does being in a group mean? In the modem community being in a group is supposed to mean that the people in the group work on projects together and trade specific information that people outside of the group are not allowed to access and by the same token, have no way to get it. However, obviously the people in the group all feel that the other people with whom they are sharing information, can be trusted and are worthy of associating with them to begin with. So when you stop and think about it, if there was no group, the people in question would still be trading information and would still trust each other because they would not have formed the group unless this criteria was met in the first place. So in truth, being in a group really means nothing on the basis previously mentioned.

You see in the modem community, being in a group really is more like a power trip or a "security blanket" for people who feel that they need to let people know that they associate with a specific clique in the hopes that the popularity of some of the other members will lend popularity to themselves.

Many groups form in such a way that they try to make it look otherwise and thus begins the real problem. Some groups are formed by a person who tries to get a lot of guys together that he feels knows a lot or seems to post a lot of good information - Bad Move; If you are going to form a group at all, stick with people who you know can be trusted (can you really ever "know" who can be trusted?) and then out of those people form your group or choose who you feel should be in it.

Anyway, to prove that they are elite, most groups begin to gather specific data for giving to group members, and this includes handing out their own names and phone numbers with other members of the group. They feel a false loyalty and psychologically create such utter faith in all the members that the faith is ultimately blind and based on hopes and aspirations of greatness.

What is the best way for a security agent or informant to blend in with the modem community? Join as many groups as possible, start gathering data on the members, and spread your handle throughout the community to become "well known."

Example: Taken From Phrack World News Issue XV;

[This article has been edited for this presentation. -KL]

- -

Mad Hatter; Informant? July 31, 1987
~~~~~~~~~~~~~~~~~~~~~~

We at Phrack Inc. have uncovered a significant amount of information that has led us to the belief that Mad Hatter is an informant for some law enforcement organization.

When Taran King, Cheap Shades, Forest Ranger, and Knight Lightning arrived at Control C's in Chicago, Illinois, Mad Hatter had already searched the place and had found some papers that could only have done ^C harm. We destroyed this information and thought everything was ok. However, as it turns out, we searched Mad Hatter's bags and found a duplicate set of this information and the general hypothesis was they he intended to leave it behind as incriminating evidence.

Mad Hatter had also brought down several disks for the purpose of copying Phantasie Realm. Please note; PR was an IBM program and MH has an apple.

Control C told us that when he went to pick Mad Hatter up at the bus terminal, he watched the bus pull in and saw everyone who disembarked. Suddenly Mad Hatter was there, but not from the bus he was supposed to have come in on. In addition to this, he had baking soda wrapped in a five dollar bill that he tried to pass off as cocaine. Perhaps to make us think he was cool or
~~~~~~~~~~~~~~~~~~~~~~

something.

Mad Hatter constantly tried to get left behind at ^C's apartment for unknown reasons. He also was seen at a neighbor's apartment making unauthorized calls into the city of Chicago. When asked who he called, his reply was "Don't worry about it." Mad Hatter had absolutely no money with him during PartyCon (and incidentally he ate everything in ^C's refrigerator) and yet he insisted that although he had taken the bus down and had return trip tickets for the bus, that he would fly back home. How was this going to be achieved? He had no money and even if he could get a refund for the bus tickets, he would still be over $200 short. When asked how he was going to do this, his reply was "Don't worry about it."

On Saturday night while on the way to the Hard Rock Cafe, Mad Hatter asked Control C for the location of his computer system and other items 4 times. This is information that Hatter did not need to know, but perhaps a SS agent or someone could use very nicely.

When Phrack Inc. discovered that Dan The Operator was an FBI informant and made the news public, several people were criticizing him on Free World II Private. Mad Hatter on the other hand, stood up for Noah and said that he was still his friend despite what had happened. Then later when he realized that people were questioning his legitimacy, his original posts were deleted and he started saying how much he wanted to kill Dan The Operator and that he hated him.

Mad Hatter already has admitted to knowing that Dan The Operator was an FBI informant prior to SummerCon '87. He says the reason he didn't tell anyone is because he assumed we already knew.

- -

When Mad Hatter first entered the phreak/hack world, he joined;

Phreaks Anonymous World Wide (PAWW),
MetalliBashers, Inc (MBI),
Order of The Rose, and
Cult of The Dead Cow (-cDc-).

If you were a security agent or a loser hacker turned informant and you wanted to mix in with the phreak/hack community, wouldn't you try to join as many groups as possible to spread your name?

- -

Phreaks Anonymous World Wide, MetalliBashers, Inc., Order of The Rose, and Cult of The Dead Cow, not exactly the toughest groups to join and once there is one security person in the group, he is bound to vouch for others, etc. So while he spreads his name as an elite modem user throughout the community, he is busy gathering information on group members who are foolish enough to trust him.

Its not bad enough that some groups are easy enough to infiltrate as it is, but does anyone remember this?

Taken From Phrack World News Issue XI;

- -

Phortune 500: Phreakdom's Newest Organization February 16, 1987
~~~~~~

For those of you who are in the least bit interested, Phortune 500 is a group of telecommunication hobbyists who's goal is to spread information as well as further their own knowledge in the world of telecommunications. This new group was formed by:

Brew Associates / Handsomest One / Lord Lawless / The Renegade Chemist
Quinton J. Miranda / Striker / The Mad Hacker / The Spiker

These eight members are also known as Board Of Directors (BOD). They don't claim to be *Elite* in the sense that they are they world's greatest hacker, but they ARE somewhat picky about their members. They prefer someone who knows a bit about everything and has talents exclusive to him/herself.

One of the projects that Phortune 500 has completed is an individual password
~~~~~~

AE type system. It's called TransPhor. It was written and created by Brew Associates. It has been Beta tested on The Undergraduate Lounge (Sysoped by Quinton J. Miranda). It is due to be released to the public throughout the next few months.

Phortune 500 has been in operation for about 4 months, and has released two newsletters of their own. The Phortune 500 Newsletter is quite like the "People" of contemporary magazines. While some magazines cover the deep technical aspects of the world in which we communicate, their newsletter tries to cover the lighter side while throwing in information that they feel is "of technical nature." The third issue is due to be released by the end of this month.

- -

>=-> The Phortune 500 Membership Questionnaire <-=<

Note: The following information is of a totally confidential nature. The reason you may find this so lengthy and in depth is for our knowledge of you. We, with Phortune 500, feel as though we should know prospective members well before we allow them into our organization. Pending the answers you supply us, you will be admitted to Phortune 500 as a charter member. Please answer the following completely...

.....

Handle :
First Name :
Voice Phone Number :
Data Phone Number :
City & State :
Age :
Occupation (If Applicable) :
Place of Employment (Optional) :
Work Phone Number (Optional) :
Computer Type :
Modem Type :
Interests :
Areas Of Expertise :
References (No More Than Three) :
Major Accomplishments (If Any) :

.....

Answer In 50 Words Or Less;

^*^ What Is Phortune 500 in Your Opinion?

^*^ Why Do You Want To Be Involved With Phortune 500?

^*^ How Can You Contribute to Phortune 500?

.....

Please answer each question to the best of your ability and then return to any Phortune 500 Board of Directors Member Or a Phortune 500 BBS:

The Private Connection (Limited Membership) 219-322-7266
The Undergraduate AE (Private Files Only) 602-990-1573

- -

An actual application form for joining a group. Perhaps the concept was a good one, perhaps not, but from a standpoint of publicity and security, this was a complete and utter catastrophe.

Basically we are all here to learn in one way or another. Groups and clubs in our community only seem to segregate it and at a time when everyone should be pulling together, this is not such a good idea. Privacy and security are important factors that motivate these sects within the society, but ultimately are the final consequences worth the trouble of creating a group?

If groups had not been created, there would not be as much attention on the phreak/hack community as there is right now. When group names start spreading, it starts the law enforcement agencies into a panic that its big time organized crime. This allows them to justify more time and money into the apprehension of computer criminals and usually they go after the big names; the people in

the most "elite" groups.

Now before you, a member of a group, start criticizing this file, please understand, I am not referring to any particular groups here, just groups in general. Any and all comments made about MBI, -cDc-, PAWW, OOTR, and P500 should not be taken personally and were used only as examples of how groups can be potential security problems.

There are some groups that are worthwhile organizations and its obvious because that have existed through the years and been productive. However, the only way to keep this community alive is for everyone to work together to protect and learn from each other.

:Knight Lightning

"The Future Is Now"

=-=

==Phrack Inc.==

Volume Two, Issue 23, File 4 of 12

Utopia

Chapter One of The Future Transcendent Saga

An Introduction To The World Of Bitnet

Presented by Knight Lightning
January 1, 1989

Special Thanks To Jester Sluggo

Welcome To The Next MILLENNIUM Of The Communications Realm
The Future is NOW!

As most people will agree, college and university computers are the easiest to gain access to, both legally and illegally. Bitnet is only one of the many interconnected wide area networks, but I felt that it was the most important to discuss because all major colleges and universities are connected by it and as such creating an almost utopian society for the technologically inclined. It's free, legal, and world encompassing -- anything that incorporates "free" with "legal" and is useful has to hold some sort of perfection and thus the name of this file.

For the people already on Bitnet, this file may seem somewhat basic and most likely contains information that you are thoroughly aware of, but you never w know what a little extra reading might lead you to discover. Once again welcome to the future... a future where limits are unknown.

:Knight Lightning

- -

The Origin Of BITNET

by Jester Sluggo

In 1981, the City University of New York (CUNY) surveyed universities on the east coast of the United States and Canada, inquiring whether there was interest in creating and easy-to-use, economical network for interuniversity communication between scholars. The response was positive. Many shared the CUNY belief in the importance of computer-assisted communication between scholars. The first link of the new network, called Bitnet, was established between CUNY and Yale University in May 1981. The term BITNET is an acronym that stands for "Because It's Time NETwork."

The network technology chosen for Bitnet was determined by the availability of the RSCS software on the IBM computers at the initial sites. The RSCS is simple and effective, and most IBM VM/CMS computer systems have it installed for local communications, supporting file transfer and remote job entry services. The standard Bitnet links are leased telephone lines running 9600 bps. Although the initial nodes were IBM machines in university computers centers, the network is in no way restricted to such systems. Any computer with an RSCS emulator can be connected to Bitnet. Emulators are available for Digital Equipment Corporation VAX/VMS systems, VAX-UNIX systems, and for Control Data Corporation Cyber systems and others. Today, more than one-third of the computers on Bitnet are non-IBM systems.

There is also some talk in the Bitnet scientific community of a merger between Bitnet and CSnet (Computer Science Network). It is unknown when or if such a merger will take place, but it is only a step in the right direction.

Note: NetNorth is the Canadian division of Bitnet and EARN is the European division of Bitnet. They are all directly connected and together serve as one network and not three. It is often referred to as BITNET/NetNorth/EARN.

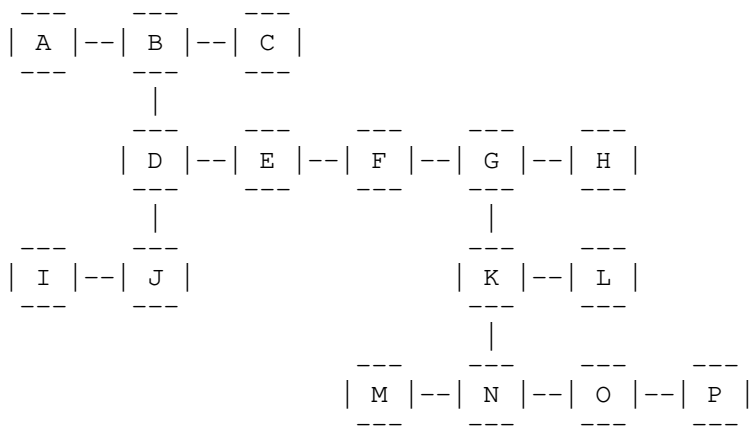
The Basics Of Bitnet
~~~~~~~~~~~~~~~~~~~~

In order to make any sense out of this file, you should first have a basic understanding of mainframes and userids, etc. Since most readers of Phrack are computer enthusiasts, there is a pretty good chance that you understand these things already. If not, you may want to find documentation on the topic. The Mentor's Beginning Hackers Guide, which was published in Phrack Inc. XXII contains some information that might help you. The concepts presented in this file are not terrible difficult to understand, but you should not jump into this totally unprepared either.

You should also be a little familiar with the type of hardware and operating system you will be using. Most IBM systems in Bitnet run VM/CMS. The Digital Equipment Corporation (DEC) VAX systems usually run an operating system called VMS along with a software package called JNET which allows them to communicate via Bitnet. I will be referring to VM/CMS and VMS/JNET throughout this file. I myself currently use an IBM 4381 that runs VM/CMS and thus I am much more familiar with that type of system.

Try to think of the mainframe as the telephone and Bitnet as the telephone lines. You see, the mainframe you log onto is connected to mainframes at other universities and institutions. The connection is usually a high-speed leased line, a special sort of telephone connection. In a way, these computers are always on the phone with each other (except when links go down, discussed in the section on MESSAGES). This particular network is what is known as a "store and forward" network. This means that if I send something to someone in Los Angeles, the computers in the network between New York and California will store and forward it from computer to computer until it reaches it's destination.

In Bitnet, there is only one way from "Point A" to "Point B." A small piece of the network might look like this:



Those boxes represent computers in the network, and the dashes between them are the leased lines. If I am at computer "A" and I send a file to someone at computer "N" it would travel the following path:

A-B-D-E-F-G-K-N

Actual topology maps are available for download from LISTSERV@BITNIC, but we will be discussing servers later in this file. Like I mentioned before, there is only one route between any two nodes and there is simply no way to bypass a disconnected link.

Each of the computers in BITNET is called a "node" and has a unique name that identifies it to the other nodes. For example, one of the mainframe computers at the University Of Missouri-Columbia has the nodename UMCVMB. So what does that mean exactly? Well in this case, UMC comes from the name of the school,
~~~~~~~~~~~~~~~~~~~~

VM comes from the Virtual Memory operating system, and B is just an alpha-numerical identifier. At one time there was a UMCVMA, but that system was taken down a couple of years ago. One thing to note here is that although this particular node can be broken down into its parts, many nodes do not follow this pattern and some nodes have "aliases." An alias is just another name for the node and both names are recognized by all Bitnet facilities. An example of this is STANFORD. The nodes STANFORD and FORSYTHE are the same place so...

CYPHER@STANFORD = CYPHER@FORSYTHE

Your userid in combination with the name of your node is your "network address." It is usually written in the format userid@node (read "userid at node"). For example, the name of my node is UMCVMB, and my userid is C483307. Therefore, my network address is C483307@UMCVMB. If I know the userid@node of someone in the network, I can communicate with that person, and he/she can communicate with me. I have found many interesting people on the networks. Making use of the direct chatting capabilities of Bitnet I am able to talk to them in "real-time." You can do this too, all you need to know are a few commands. This is explained in part two.

Messages

There are three basic methods of communicating via Bitnet: MAIL, MESSAGE, and FILE. The reason you would choose one over the other for a particular application will become clear after a little explanation.

The MESSAGE is the fastest and most convenient method of communication available through Bitnet. It is the network's equivalent of a telephone conversation. The difference of course is that the words are typed instead of spoken. The message you type is transmitted immediately (well, quickly) to its destination. In BITNET this destination is the network address (userid@node) of the person you want to contact. If the person you are contacting is logged on, the message will be displayed on their screen. If not, their computer will tell you so by sending you a message. In this case, your message is lost forever. In other words, no one is there to answer the phone. However, many people run a program called GONE (and there are other similar programs) which acts like an answering machine and holds your message until they log on. Some universities do not allow this program because it uses a lot of CPU time. If your school or mainframe does not allow it, do not try to sneak its use, because it is very easy to detect.

One important thing to mention is that not all nodes allow interactive chat. Some nodes are simply not advanced enough for it and you will a receive a message telling you this whenever you try to chat with them. However, this situation is less common.

The command to send messages depends on your computer and system software. People on VM/CMS systems would type something like this:

```
TELL userid AT node message OR TELL userid@node message
```

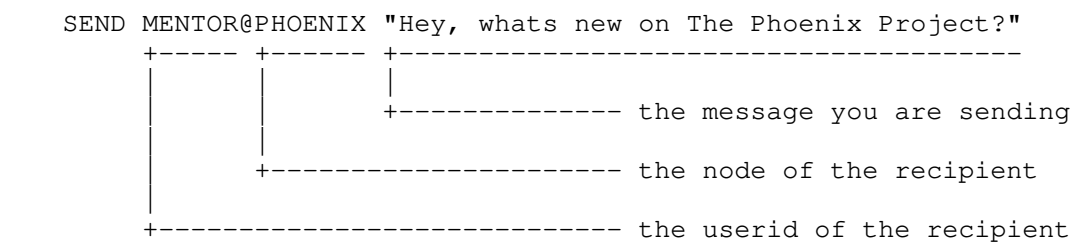
For example:

```
TELL MENTOR AT PHOENIX Hey, whats new on The Phoenix Project?
     +-----    +------ +-------------------------------------
     |         |       |
     |         |       +----------- the message you are sending
     |         |
     |         +------------------- the node of the recipient
     |
     +----------------------------- the userid of the recipient
```

People on VAX/VMS systems using the JNET networking software would use this syntax:

```
SEND userid@node "message"
```

For example:



The quotes around the message are optional. However, the JNET networking for VAX/VMS will translate your entire message into upper-case characters if you DO NOT use them. Many people find receiving messages in all upper case to be extremely annoying.

For more information on the TELL and SEND commands, you should consult your local system documentation.

When a message arrives on your screen, it will look something like this:

```
FROM PHOENIX(MENTOR):  Hello!  Things are great here, you?
```

Unfortunately there is a downside to everything and Bitnet Messages are no exception. Text sent by message must be short. In general, your message length can be one line, about the width of your screen. In other words, you won't be sending someone a copy of Phrack World News via the TELL command.

Also, you can only communicate with someone in this way when they are logged on. Considering time zone differences (you may find yourself talking to people in Europe, Israel, or Australia) this is often quite inconvenient.

Lastly, there is the problem of links that I call LinkDeath. If the connection to the node you want to contact is broken (by for example, a disconnected phone line), you'll receive an error message and whatever you sent is gone. This can be very annoying if it should occur during a conversation. The LinkDeath may last a few minutes or several hours. Often times, a link will go down for the weekend and you are simply out of luck. Even worse is when it is the link that connects your mainframe to rest of Bitnet... you are cut off.

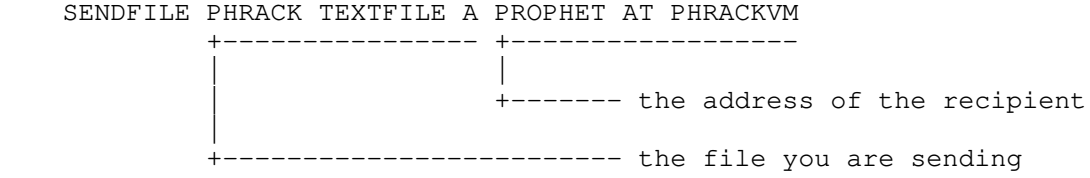
However, messages are very far from useless. As I will demonstrate in chapter two, TELL and SEND are extremely helpful in accessing the many servers on Bitnet.

Files

FILES are another way to communicate over Bitnet. The text files and programs that you store on your computer can be transmitted to users at other nodes. This is one of the methods that I use to distribute Phrack issues across not only the country, but the world. People on VM/CMS systems would use a syntax like this:

```
SENDFILE filename filetype filemode userid AT node
```

For example:



However, at my particular node the command would read:

```
SENDFILE PHRACK TEXTFILE A TO (nickname)
```

For some reason at my node, you cannot use SENDFILE to send a file to anyone unless they are in your NAMES file. The NAMES file is a database type of list that translates userid@node into nicknames to make it easier to chat with people. This way you can use their nickname instead of the tiresome userid@node. The filemode, in this example "A", is the disk that the file "PHRACK TEXTFILE" is on. In case you were wondering, with the exception of my address, most of the addresses in this file like PROPHET@PHRACKVM or MENTOR@PHOENIX are bogus and just examples for this presentation.

The syntax for VMS/JNET systems is quite similar:

```
SEND/FILE filename.extension userid@node
```

For example:

```
SEND/FILE PHRACK.TEXTFILE PROPHET@PHRACKVM
          +--------------- +---------------
          |                |
          |                +-------- the address of the recipient
          |
          +------------------------- the file you are sending
```

The file sent is stored in the "electronic mailbox" of the recipient until he/she logs on. People on VM/CMS systems would use the RECEIVE or RDRLIST (shortened to "RL") commands to process files sent to them in this way. People on VAX/VMS systems would use the RECEIVE command. You should check your local documentation for more information on these commands.

SEND/FILE and SENDFILE are useful for sending programs or large volumes of data like Phrack issues over the network. However, they should not be used for everyday communication because there is a much easier way -- the MAIL.

Mail

The other form of Bitnet communication has been given a very apt name: MAIL (often called "electronic mail" or "e-mail"). Just like regular postal service mail, you provide an address, return address, and text. Software for sending mail software differs from site to site, so you will have to look in your local documentation for information. On my particular node, the return address (your address) is automatically placed in the letter. This presentation should be able to shed some light on what most mail looks like and how it works.

Mail files are really just specially formatted text files. The feature that makes them different is the "mail header." This tells a Bitnet system and your mail software that it is not a regular text file. It looks something like this:

```
                                          The address of the recipient
                                                                     |
                                                        The subject  |
                                                                  |  |
                                                  Your address    |  |
                                                               |  |  |
                                               Todays date     |  |  |
                                                            |  |  |  |
Date:         Fri, 29 Dec 88 23:52:00 EDT                <--+  |  |  |
From:         Forest Ranger <RANGER@STLVAX1>             <-----+  |  |
Subject:      Cable Pair Busted For Child Molestation    <--------+  |
To:           Phrack World News <KNIGHT@MSPVMA>          <-----------+
```

An entire mail message would look like this:

```
+---------------- Mail header
|
|  Date:         Fri, 29 Dec 88 23:52:00 EDT
|  From:         Forest Ranger <RANGER@STLVAX1>
```

```
  |  Subject:      Cable Pair Busted For Child Molestation
  |  To:           Phrack World News <KNIGHT@MSPVMA>
  +  ========================================================================

  +  Have you seen the newspapers?  Is this good news, or what?  I think that
  |  the ramifications are startling.  This is one more step on the road to a
  |  higher civilization.  I hope he gets what he deserves.  Keep in touch, I
  |  will send more information later.
  |
  +---------------- Mail text
```

Mail has a number of advantages. The size of a mail file is limited only by you and is the only way to send files to networks other than Bitnet (However, I do not recommend that you transmit anything longer than 3000 lines). When your mail reaches the destination address, it will be stored in the user's mailbox until they read it. If the links to that particular node are disconnected, your mail will be held until the path is clear for the mail to continue on its route to the recipient's mailbox.

The disadvantage of mail is that it is, indeed, slower than messages. The longer your mail file, the longer it will take to get from Point A to Point B.

Conclusion
~~~~~~~~~~

Don't despair, this is only the conclusion to this file. The best functions of Bitnet are yet to be described. Join me in the second chapter of The Future Transcendent Saga -- Foundations Upon The Horizon.

Also included in this issue of Phrack are sitelists for Bitnet. Actual node directories are available from LISTSERV@BITNIC, but they are much too large to be printed here. However, the files that are included list the names of the universities and institutions that are connected to Bitnet without their node addresses (some institutions have over 30+ nodes). If you attend a college or university that is hooked into Bitnet, then join me in the realm of infinite discovery. When you do, drop me a line...

:Knight Lightning (C483307@UMCVMB)

For related reading please see;

An Insight On Wide-Area Networks Part 2 by Jester Sluggo
(Phrack Inc. Issue 6, file 8)

Communications Of The ACM

~~~~~~~~~~

==Phrack Inc.==

Volume Two, Issue 23, File 5 of 12

Foundations Upon The Horizon

Chapter Two of The Future Transcendent Saga

Using Servers And Services In The World Of Bitnet

Presented by Knight Lightning
January 2, 1989

Welcome to the second chapter of The Future Transcendent Saga. In this file, I will present the servers and services of Bitnet (although there are some services and servers on other networks as well). You will learn what the servers are, how they differentiate, how to use them, and come to a better understanding of how these Foundations Upon The Horizon help make Bitnet a virtual Utopia.

What Is A Server?

One of most useful features of Bitnet is the variety of file servers, name servers, relays, and so on. They might be described as "virtual machines" or "server machines."

A "server" is a userid a lot like yours. It may exist on your computer (node) or on some other BITNET node. The people who set up this userid have it running a program that will respond to your commands. This is a "server." The commands you send and the way in which the server responds to them depends on the particular program being run. For example, the servers UMNEWS@MAINE and 107633@DOLUNI1 offer different types of services, and require different commands. The various kinds of servers are described later in this document.

You can send your commands to most servers in one of two formats: MAIL or MESSAGE.

Not all servers accept commands via both formats, but this information is included in the document BITNET SERVERS which can be obtained from LISTSERV@BITNIC. Because there are so many servers I will not even begin to list them here. Different servers are created and disconnected everyday so it would be difficult to name them all.

People on VM/CMS systems would send commands something like this:

```
TELL userid AT node command   (AT = @)
```

For example:

```
TELL NETSERV@MARIST HELP
```

People on VAX/VMS systems using the JNET networking software would use this syntax:

```
SEND userid@node "command"
```

For example:

```
SEND NETSERV@MARIST "HELP"
```

Many servers can also accept commands via mail. Indeed, some will only accept your commands in that format, such as the servers on the non-Bitnet nodes. The syntax for the commands you send remain the same. You send mail to the server as if you were sending the mail to a person. The text of your message would be

the command. Some servers will take the command as the first line of a text message, others require it in the "Subject:" line. Some servers will accept more than one command in a mail message, others will take only one. Here is an example of a mail message sent to LISTSERV@BITNIC requesting a list of files:

```
Date:         Fri, 30 Dec 88 23:52:00 EDT
From:         Taran King <SYSOP@MSPVMA>
To:           Listserv <LISTSERV@BITNIC>
========================================================================
INDEX
```

Throughout this file I will use examples where commands are sent to servers via message. However, for many of the cases we will present you have option of using mail. The choice is yours.

There are two particularly confusing aspects of servers of which you should be aware. First, servers in the same category (say, file servers) do not always accept the same commands. Many of them are extremely different. Others are just different enough to be annoying. There are many approaches to setting up a server, and everyone is trying to build a better one.

The second problem is that there are many servers that fill two, sometimes three categories of server. For example, LISTSERV works as a list server and a file server. Many LISTSERVs have been modified to act as name servers as well, but they are rather inefficient in this capacity. If you do not understand this terminology, bear with me. The best is yet to come.

File Servers

Remember that a server runs on a userid much like yours. Like your userid, it has many capabilities, including the ability to store files (probably with a much greater storage capacity though). The program that a file server runs enables it to send you files from its directory, as well as a list of files available. These may be programs or text files. You might look at these servers as Bitnet versions of dial-up bulletin boards or AE Lines.

You can generally send three types of commands to a file server. The first type is a request for a list of files the server offers. The second is a request that a specific file be sent to your userid. The third, and most important is a HELP command.

The HELP command is very important because it is one of the few commands that almost all servers accept, no matter what the type. Because the commands available differ from server to server, you will often find this indispensable. Sending HELP to a server will usually result in a message or file sent to your userid listing the various commands and their syntax. You should keep some of this information handy until you are comfortable with a particular server.

To request a list of files from a server, you will usually send it a command like INDEX or DIR. The list of files will be sent to you via mail or in a file. For example:

```
VM/CMS:      TELL LISTSERV@BITNIC INDEX
VMS/JNET:    SEND LISTSERV@BITNIC "INDEX"
```

To request a specific file from the list you receive, you would use a command like GET or SENDME. For example to request the file BITNET TOPOLOGY from LISTSERV@BITNIC you would type on of the following:

```
VM/CMS:      TELL LISTSERV@BITNIC SENDME BITNET TOPOLOGY
VMS/JNET:    SEND LISTSERV@BITNIC "SENDME BITNET TOPOLOGY"
```

In many cases the files are organized into subdirectories or filelists. This can make requesting a file more complicated. This makes it even more essential that you keep documentation about a particular server handy. Some file servers offer programs that you can run which will send commands to the server for you.

Name Servers

Name servers serve two purposes; to assist you in finding an address for someone or to help you find people with specific interests. I doubt you are going to care about tracking down people by their interests, so I am not going to discuss those aspects of nameservers. The servers that actually let you look up people are few and far between. Because there are so few I have composed this list;

Columbia University	FINGER @ CUVMA
Cork University	INFO @ IRUCCIBM
Drew University	NAMESERV @ DREW
North Dakota State University	FINGER @ NDSUVM1
Ohio State University	WHOIS @ OHSTVMA
Pennsylvania State University	IDSERVER @ PSUVM
Rochester Institute Of Technology	INFO @ RITVAXD
	LOOKUP @ RITVM
State University of New York (SUNY) at Albany	WHOIS @ ALBNYVM1
University of Calgary	NAMESERV @ UNCAMULT
University of Kentucky	WHOIS @ UKCC
University of Illinois at Urbana-Champagne	PHSERVE @ UIUCVMD
University of Louisville (Kentucky)	WHOIS @ ULKYVM
University of Regina	VMNAMES @ UREGINA1
University of Tennessee	UTSERVER @ UTKVM1
Weizmann Institute of Science	VMNAMES @ WEIZMANN

So as not to be misleading, these servers do not necessarily cover the entire school. Example: The server at University of Louisville covers people on the node ULKYVM, but not the nodes ULKYVX0x (x = 1 - 8 I believe). ULKYVX is a VAXcluster of nodes at University of Louisville, but the people on those systems are NOT indexed on the server at ULKYVM. In contrast, the nameserver at University of Illinois contains online listings for every student and staff member whether they have accounts on the computer or not. You can get phone numbers and addresses using this. Please note that the above list is only to the best of my knowledge and others may exist.

There are also many Listservs that have a command to search for people, but with Listserv, signing up is by choice and not mandatory. You also will end up getting listings for people from nodes other than the one you are searching.

Ok, lets say I am trying to find an account for Oryan QUEST and I am told by a friend that he is going to school at Ohio State University. Ohio State University has a nameserver and if he has an account on their computer I should be able to find him.

```
VM/CMS:      TELL WHOIS@OHSTVMA Quest
VMS/JNET:    SEND WHOIS@OHSTVMA "Quest"
```

This particular nameserver only requires that you enter the persons name with no "search" command. Some servers require this. Your best bet is to send the command "HELP" first and you'll receive documentation.

Ok, back to the example... unfortunately, there is no entry for "Quest" and I am out of luck. I should have been smart enough to realize that no college would be likely to let Oryan QUEST enroll in the first place -- my mistake.

In any case, I highly recommend that you register yourself with UMNEWS@MAINE and BITSERVE@CUNYVM. These are popular nationwide servers that are often used to locate people.

Forums, Digests, and Electronic Magazines

The concept of mailing lists has been given new life with the creation of computer networks. Let me explain what I mean. Almost everyone is on some sort of mailing list; magazines, bills or even pamphlets from your congressman.. The computer networks have brought a whole new degree of speed and functionality to mailing lists, as you will see.

In Bitnet, mailing lists are used mainly to keep people with similar interests in contact. There are several formats in which this contact can take place. These are "forums," "digests," and "electronic magazines".

FORUMS are a good example of how the utility of mailing lists has been expanded in Bitnet. Let's say that you have subscribed to a forum for people interested in Cyberpunks. How you could subscribe to such a list will be described later. Another person on the mailing list sends mail to a server where the list is kept. This server forwards the mail to all of the people in the forum. When mail from a forum arrives in your computer mailbox, the header will look much like this:

```
Date:         Fri, 10 Sep 88 23:52:00 EDT
Reply-To:     CYBER Discussion List <CYBER-L@PUNKVM>
Sender:       CYBER Discussion List <CYBER-L@PUNKVM>
From:         Sir Francis Drake <DRAKE@WORMVM>
Subject:      Invasion From X-Neon!
To:           Solid State <SEKER@PLPVMA>
=========================================================================
```

This may look a little confusing, but there really isn't much to it. In this example, Sir Francis Drake ("From:") sent mail to the CYBER-L list address. This server then forwarded the mail to everybody on the list, including Solid State ("To:"). Note the line named "Reply-To:". This line tells your mail software that when you reply to the note (if you reply) that the reply should go to the list... meaning *everybody* on the list. People will in turn reply to your mail, and you have a forum.

Some forums are very interesting, but using the digests can lead to problems. First among these is the volume of mail you can receive. If you are in a very active forum, you can get 50 or more pieces of electronic mail in a single day. If you are discussing a controversial or emotional topic, expect more.

Many people have a tendency to "flame" (the Bitnet term for ragging). The speed and immediacy of electronic mail makes it very easy to whip out a quick, emotional response, to which there will be similar replies. I advise you to take some time and think out your responses to forum postings before inadvertently starting a "flame war." Hopefully anyone able to gain access to college computers will be mature enough to have outgrown these battles.

DIGESTS provide a partial solution to the these problems. In this case, mail that is sent to a mailing list is stored rather than sent out immediately. At some point the "Moderator" for the list organizes and condenses all of the correspondence for the day or week. He then sends this out to the people on the mailing list in one mailing.

The drawback with this setup is that it requires a lot of human intervention. If the moderator gets sick, goes on vacation, or quits, activity for a particular digest can come to a screeching halt.

ELECTRONIC MAGAZINES take the digest concept a step further. These mailing lists actually duplicate the organization and format of "real" magazines. Bitnet is used as a convenient and inexpensive distribution method for the information they contain. The frequency of distribution for these electronic magazines ranges ranges from weekly to quarterly to "whenever the editor feels like it" (sort of like Phrack releases). This is the most formal, structured form of Bitnet communication. Where a digest is simply a group of letters organized by topic, an electronic magazine includes articles, columns, and features. Perhaps the only feature of paper magazines that they do *not* include is advertisements. Bitnet NetMonth and NetWeek are two of the better magazines on Bitnet and they contain useful information if you know what you're looking for. I will discuss how to subscribe to these magazines as well as the other forms of media in the next part of this file.

List Servers

In the previous section, I mentioned that some servers are used to control mailing lists. A server that performs this function is called a "list server."

Almost all of these listservers have the userid of LISTSERV, such as LISTSERV@BITNIC. One of these servers can control subscriptions to many mailing lists. The other concept behind Listservs are the list-ids, but as these are rather unimportant and vary from server to server I am not going to discuss them here. If you would like to learn about these, consult your local listserv and request documentation with the HELP command.

To subscribe to a mailing list, you would send a LISTSERV a SUBSCRIBE command, which has the following syntax:

SUBscribe listname (whatever name you want)

In this example, SpyroGrya is sending LISTSERV@BITNIC the command to subscribe to ETHICS-L:

VM/CMS: TELL LISTSERV@BITNIC SUB ETHICS-L SpyroGyra
VMS/JNET: SEND LISTSERV@BITNIC "SUB ETHICS-L SpyroGyra"

If you misspell your name when entering a SUBscribe command, simply resend it with the correct spelling. To delete his name from the mailing list, SpyroGyra would enter an UNSUBscribe command:

VM/CMS: TELL LISTSERV@BITNIC UNSUB ETHICS-L
VMS/JNET: SEND LISTSERV@BITNIC "UNSUB ETHICS-L"

In many cases the SIGNOFF command is used instead of UNSUB, but those are the basic commands you need to know in order to access Listserv controlled mailing lists. However, Listserv has a multitude of features, so it would be a good idea to read the Listserv documentation.

Note If you are on a VAXcluster, you should send SUBSCRIBE and UNSUBSCRIBE commands to LISTSERV via MAIL.

Relays

Relay might be one of the easier types of servers to understand. If you have used the CB Simulator on CompuServe or are familiar with Diversi-Dials (or maybe even ALTOS Chat) you will catch on to the concept quickly. The idea behind Relay is to allow more than two people to have conversations by interactive message. Without Relay-type servers, this would not be possible.

Let’s set up a scenario:

Sluggo, Taran, and Mentor are at different nodes. Any two of them can have a conversation through Bitnet. If the three of them want to talk, however, they have a problem. Sluggo can send Mentor messages, but Taran can’t see them. Likewise, Taran can send Sluggo messages, but then Mentor is in the dark. What they need is a form of teleconferencing. Alliance doesn’t exist on Bitnet so they created Relays.

Each of these users "signs on" to a nearby Relay. They can pick a channel (0-999 although there are more, but they are reserved for special use). Instead of sending messages to Taran or Sluggo, Mentor sends his commands to the Relay. The Relay system then sends his message to *both* Taran and Sluggo. The other users can do the same. When they are done talking, they "sign off."

Relays can distinguish commands from the text of your messages because commands are prefixed with a slash "/". For example, a HELP command would look like this:

VM/CMS: TELL RELAY@UIUCVMD /HELP
VMS/JNET: SEND RELAY@UIUCVMD "/HELP"

A message that is part of a conversation would be sent like so:

VM/CMS: TELL RELAY@UIUCVMD Hello there!
VMS/JNET: SEND RELAY@UIUCVMD "Hello there!"

When you first start using Relay, you must register yourself as a Relay user

using the /SIGNUP or /REGISTER commands:

```
VM/CMS:      TELL RELAY@UIUCVMD /REGISTER (Choose a name)
VMS/JNET:    SEND RELAY@UIUCVMD "/REGISTER (Choose a name)"
```

They want you to use your real name, do so if you want, but they really have no way to check unless one of the operators is a user consultant at your node and looks up your account. Just use names that look real and you'll be fine.

You can then sign on. You can use a nickname or handle. In the following example, I am signing on to Channel 260 with a nickname of "KLightning":

```
VM/CMS:      TELL RELAY@UIUCVMD /SIGNON KLightning 260
VMS/JNET:    SEND RELAY@UIUCVMD "/SIGNON KLightning 260"
```

You can then start sending the Relay the text of your messages:

```
VM/CMS:      TELL RELAY@UIUCVMD Good evening.
VMS/JNET:    SEND RELAY@UIUCVMD "Good evening."
```

Relay messages will appear on your screen like this. Note the nickname near the beginning of the message. When you send conversational messages to the Relay, it automatically prefixes them with your nickname when it forwards it to the other users:

```
FROM UIUCVMD(RELAY): <Taran_King> Hello KLightning.
```

You can find out who is on your channel with a /WHO command. In the following example, someone is listing the users on Channel 260.

```
VM/CMS:      TELL RELAY@UIUCVMD /WHO 260
VMS/JNET:    SEND RELAY@UIUCVMD "/WHO 260"
```

The response from the Relay would look like this:

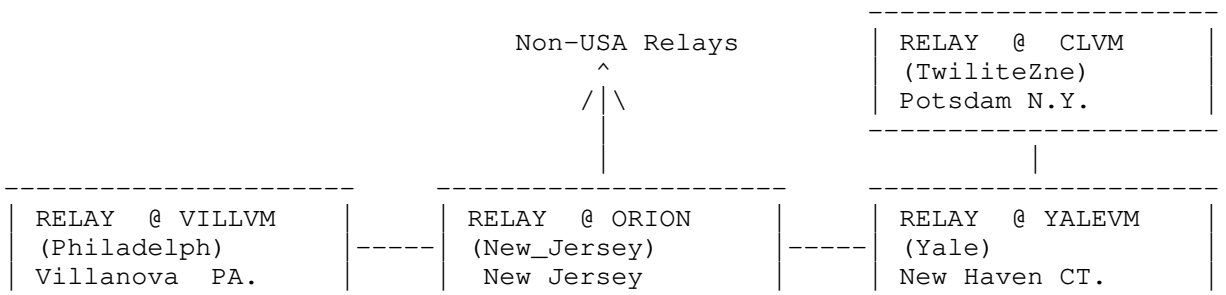
```
FROM UIUCVMD(RELAY): Ch    UserID @ Node     Nickname
FROM UIUCVMD(RELAY): 260   C483307@UMCVMB   (KLightning)
FROM UIUCVMD(RELAY): 260    MENTOR@PHOENIX  (The_Mentor)
FROM UIUCVMD(RELAY): 260   C488869@UMCVMB   (Taran_King)
FROM UIUCVMD(RELAY): 260   PROPHET@PHOENIX  (  Prophet )
FROM UIUCVMD(RELAY): 260     DRAKE@WORMVM   (   Sfd    )
FROM UIUCVMD(RELAY): 260    JESTER@NDSUVM1  (  Sluggo  )
FROM UIUCVMD(RELAY): 260       TUC@RACS3VM  (   Tuc    )
FROM UIUCVMD(RELAY): 260     VINNY@LODHVMA  (Lex_Luthor)
```

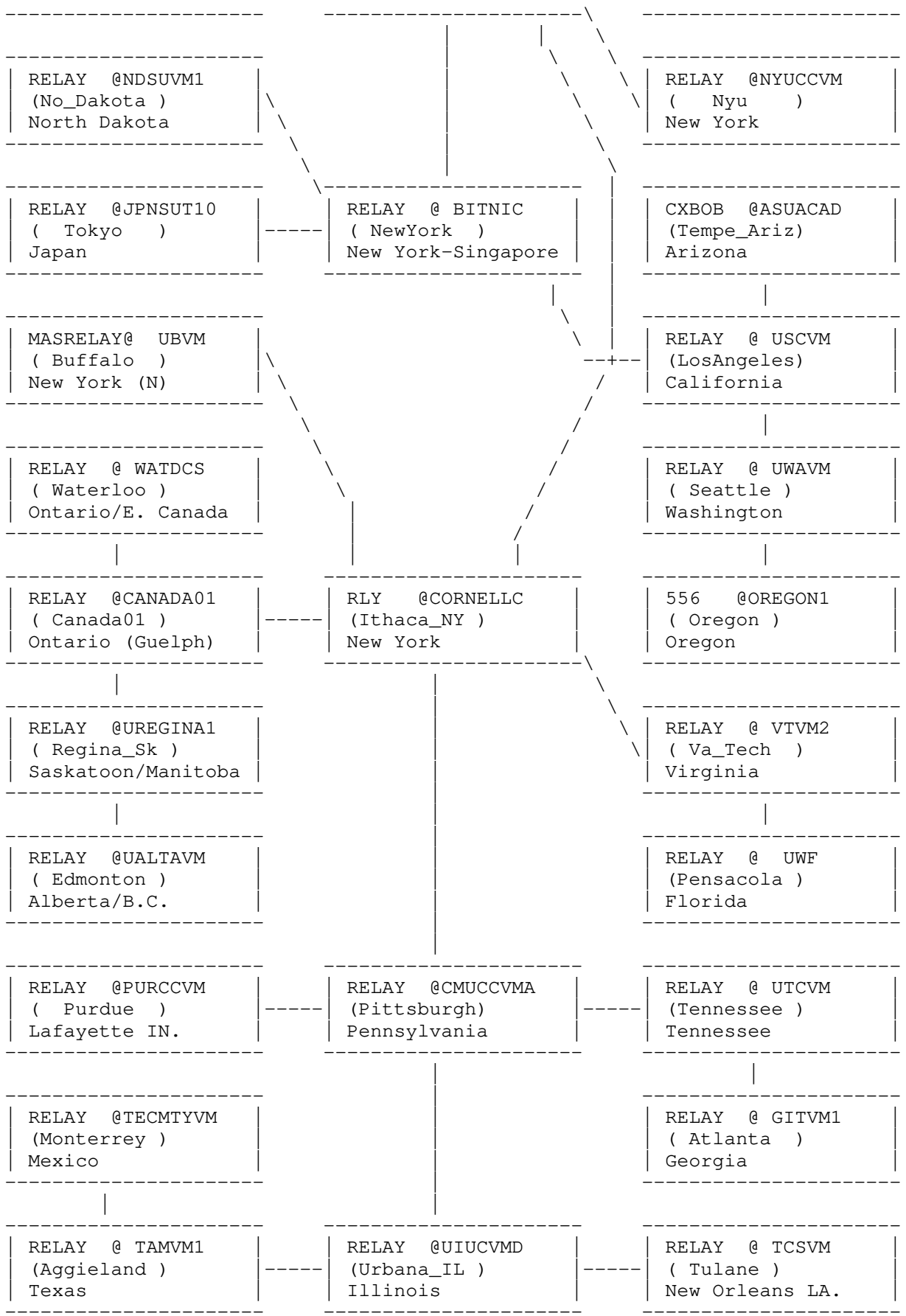
When you are done with your conversation, you can sign off the Relay:

```
VM/CMS:      TELL RELAY@UIUCVMD /SIGNOFF or /BYE
VMS/JNET:    SEND RELAY@UIUCVMD "/SIGNOFF" or "/BYE"
```

There are several commands for listing active channels, sending private messages, and so on. When you first register as a Relay user, you will be sent documentation. You can also get this information with the /INFO command. To determine which Relay serves your area, send any of the Relays listed in BITNET SERVERS the /SERVERS command. Also, because of Bitnet message and file traffic limits, many Relays are only available during the evening and weekends.

To help illustrate how the Relays work I have included this map;
[United States of America locations only]





Conclusion
~~~~~~~~~~

So what lies beyond the boundaries of Bitnet? There are many other networks that are similar to Bitnet both in function and in services. How to mail to these networks will be discussed in the next chapter of The Future Transcendent Saga -- Limbo To Infinity.
~~~~~~~~~~

:Knight Lightning

==Phrack Inc.==

Volume Two, Issue 23, File 6 of 12

```
<><><><><><><><><><><><><><><><><><><><><><><><><><><><>
<>                                                    <>
<>               UTOPIA Index File 1                  <>
<>                                                    <>
<>            BITNET Member Institutions              <>
<>                                                    <>
<>                  December 1988                     <>
<>                                                    <>
<><><><><><><><><><><><><><><><><><><><><><><><><><><><>
```

Abilene Christian University
Albion College
Allegheny College
American Assoc of State Colleges Univs (AASCU) Meeting
American Institute of Physics
American Physical Society
American University
Amherst College
Annenberg Research Institute
Appalachian State University
Argonne National Laboratory
Arizona State University
Association for Computing Machinery
Auburn University

Babson College
Ball State University
Baylor University
Bentley College
Biotechnology Research Center
BITNET Network Information Center
BITNET-Internet Gateway
Boise State University
Boston College
Boston University
Bowdoin College
Bowling Green State University
Brandeis University
Brigham Young University
Brookhaven National Laboratory
Brown University
Bryn Mawr College
Bucknell University

California Institute of Technology
California Polytechnic State University-San Luis Obispo
California State University
Canisius College
Carnegie Mellon University
Case Western Reserve University
Catholic University of America
Catonsville Community College
Central Michigan University
Chemical Abstracts Service
City University of New York CUNY
Claremont Graduate School
Clark University
Clarkson University
Clemson University
Cleveland State University
Cold Spring Harbor Laboratory
Colgate University
College of DuPage
College of the Holy Cross
College of William and Mary

Colorado School of Mines
Colorado State University
Columbia University
Columbia University Teachers College
Connecticut College
Connecticut State University System
Continuous Electron Beam Accelerator Facility
Control Data Corporation
Cornell University

Dakota State College
Dartmouth College
Davidson College
De Paul University
Denison University
Dickinson College
Drake University
Drew University
Drexel University
Duke University

East Carolina University
East Tennessee State University
Educational Computing Network of Illinois
Educational Testing Service
EDUCOM
Electric Power Research Institute
Emory University
Exxon Research and Engineering Company

Fermi National Accelerator Laboratory
Florida Central Regional Data Center
Florida Northeast Regional Data Center
Florida State University
Food and Drug Administration
Fordham University
Franklin and Marshall College
Fred Hutchinson Cancer Research Center

Gallaudet University
General Electric Corporate Research & Development
George Mason University
George Washington University
Georgetown University
Georgetown University Medical Center
Georgia Institute of Technology
Georgia State University
Gettysburg College
Grinnell College
Gustavus Adolphus College

Hampshire College
Harvard University
Harvey Mudd College
Haverford College
Hofstra University
Howard University
IBM Almaden Research Center
IBM VNET Gateway
IBM Watson Scientific Research Center Yorktown
Illinois Institute of Technology
Indiana University
Indiana University of Pennsylvania
Indiana University/Purdue University at Indianapolis
Institute for Advanced Study
Iona College
Iowa State University
Ithaca College

James Madison University

Jersey City State College
John Carroll University
John Von Neumann Center
Johns Hopkins University

Kansas State University
Kent State University

Lafayette College
Lawrence Berkeley Laboratory
Lawrence University
Le Moyne College
Lehigh University
Lewis and Clark College
Long Island University
Los Alamos National Laboratory
Louisiana State University
Louisiana State University Medical Center
Loyola College
Loyola University of Chicago

Macalester College
Macomb Community College
Manhattan College
Maricopa County Community College District
Marist College
Marquette University
Marshall University
Massachusetts Institute of Technology
Medical College of Ohio
Medical College of Wisconsin
Medical University of South Carolina
Merit Computer Network
Miami University
Michigan State University
Michigan Technological University
Middlebury College
Millersville University of Pennsylvania
Mississippi State University
Montana State University
Montgomery College
Mount Holyoke College

NASA Goddard Institute for Space Studies
National Academy of Sciences
National Aeronautics and Space Administration
National Astronomy and Ionosphere Center
National Bureau of Standards
National Center for Atmospheric Research
National Institute of Environmental Health Sciences
National Institutes of Health
National Radio Astronomy Observatory
National Science Foundation
Naval Health Sciences Education and Training Command
Naval Postgraduate School
New Jersey Educational Computer Network
New Jersey Institute of Technology
New Mexico State University
New York State College of Ceramics at Alfred University
New York University
North Carolina State University
North Dakota Higher Education Computer Network
Northeast Missouri State University
Northeastern University
Northern Arizona University
Northern Illinois University
Northwestern University
Norwich University

Oak Ridge National Laboratory

Oakland Community College
Oberlin College
Ohio State University
Ohio University
Ohio Wesleyan University
Oklahoma State University
Old Dominion University
Online Computer Library Center (OCLC)
Oregon State University

Pace University Pleasantville-Briarcliff Campus
Pacific Lutheran University
Pan American University
Pennsylvania State University
Pepperdine University
Polytechnic University
Pomona College
Portland State University
Pratt Institute
Princeton University
Purdue University

Radford University
Reed College
Regents Computer Network
Rensselaer Polytechnic Institute
Research Libraries Group
Rhodes College
Rice University
Rochester Institute of Technology
Rockefeller University
Rohm and Haas Company
Rose-Hulman Institute of Technology
Rutgers University

Saint Louis University
Saint Mary's University of San Antonio
Saint Michael's College
Saint Peter's College
Salk Institute
Sam Houston State University
Samford University
San Diego Supercomputer Center
Santa Clara University
Seton Hall University
Shriners Hospital for Crippled Children
Skidmore College
Smith College
Smithsonian Institution
South Dakota State University
Southeast Regional Data Center/FIU
Southeastern Massachusetts University
Southern Illinois University
Southern Illinois University at Edwardsville
Southern Methodist University
Southwest Missouri State University
Southwest Texas State University
Space Telescope Science Institute
St. Lawrence University
Stanford Linear Accelerator Center
Stanford Synchrotron Radiation Laboratory
Stanford University
State University of New York Agricultural and Tech College at Canton
State University of New York Agricultural & Tech Col at Farmingdale
State University of New York at Albany
State University of New York at Binghamton
State University of New York at Buffalo
State University of New York at Stony Brook
State University of New York Central Administration
State University of New York College at Brockport

State University of New York College at Buffalo
State University of New York College at Cortland
State University of New York College at Fredonia
State University of New York College at Geneseo
State University of New York College at New Paltz
State University of New York College at Old Westbury
State University of New York College at Oneonta
State University of New York College at Oswego
State University of New York College at Plattsburgh
State University of New York College at Potsdam
State University of New York College of Technology at Alfred
State University of New York College of Technology at Delhi
State University of New York Health Science Center at Brooklyn
State University System of Minnesota System Office
Stephen F. Austin State University
Stevens Institute of Technology
Swarthmore College
Syracuse University

Tarleton State University
Temple University
Tennessee Technological University
Texas A&M University
Texas Christian University
Texas Tech University
The Center for Cultural and Technical Exchange Between East and West
The Citadel, The Military College of South Carolina
The Jackson Laboratory
The World Bank
Towson State University
Transylvania University
Trenton State College
Triangle Universities Computation Center
Triangle Universities Nuclear Laboratory
Trinity College
Trinity University
Tufts University
Tulane University

Uniformed Services University of the Health Sciences
Union College
United States Environmental Protection Agency
United States Geological Survey
University of Akron
University of Alabama
University of Alabama at Birmingham
University of Alaska
University of Arizona
University of Arkansas
University of Arkansas at Little Rock
University of Arkansas for Medical Sciences
University of California
University of California Berkeley
University of California Davis
University of California Irvine
University of California Los Angeles
University of California Riverside
University of California San Diego
University of California San Francisco
University of California Santa Barbara
University of California Santa Cruz
University of Central Florida
University of Chicago
University of Cincinnati
University of Colorado at Boulder
University of Colorado at Colorado Springs
University of Colorado at Denver
University of Colorado Health Sciences Center
University of Connecticut
University of Dayton

University of Delaware
University of Denver
University of Florida
University of Georgia Athens
University of Hartford
University of Hawaii
University of Houston
University of Houston at Clear Lake
University of Idaho
University of Illinois at Urbana-Champaign
University of Illinois Chicago
University of Iowa
University of Kansas
University of Kansas Medical Center
University of Kentucky
University of Louisville
University of Maine
University of Maryland
University of Massachusetts at Amherst
University of Massachusetts at Boston
University of Medicine & Dentistry of New Jersey
University of Michigan
University of Minnesota
University of Minnesota at Morris
University of Minnesota Duluth
University of Mississippi
University of Missouri - Columbia
University of Missouri - Kansas City
University of Missouri - Rolla
University of Missouri - St. Louis
University of Nebraska - Omaha
University of Nebraska Computer Services Network
University of Nebraska Lincoln
University of Nebraska Medical Center
University of Nevada
University of New Hampshire
University of New Mexico
University of New Orleans
University of North Carolina at Chapel Hill
University of North Carolina at Charlotte
University of North Carolina at Greensboro
University of North Carolina Gen Ad Cntrl Of-Ed Cmptg Srvs
University of North Florida
University of North Texas
University of Notre Dame
University of Oklahoma Norman Campus
University of Oregon
University of Pennsylvania
University of Pittsburgh
University of Puerto Rico
University of Rhode Island
University of Richmond
University of Rochester
University of Scranton
University of South Alabama
University of South Carolina
University of Southern California
University of Southern Mississippi
University of Tennessee
University of Tennessee at Chattanooga
University of Tennessee at Knoxville
University of Tennessee at Memphis
University of Texas at Arlington
University of Texas at Austin
University of Texas at Dallas
University of Texas at El Paso
University of Texas at Houston
University of Texas at San Antonio
University of Texas Health Science Center at San Antonio
University of Texas Medical Branch at Galveston

University of Texas Southwestern Medical Center at Dallas
University of Texas System
University of the District of Columbia
University of Toledo
University of Tulsa
University of Utah
University of Vermont
University of Virginia
University of Washington
University of West Florida
University of Wisconisn - La Crosse
University of Wisconsin - Oshkosh
University of Wisconsin - Stout
University of Wisconsin Eau Claire
University of Wisconsin Madison
University of Wisconsin Milwaukee
University of Wyoming
Utah State University

Valparaiso University
Vanderbilt University
Vassar College
Villanova University
Virginia Commonwealth University
Virginia Community College System
Virginia Polytechnic Institute and State University

Washington State University
Washington University
Wayne State University
Wesleyan University
West Chester University of Pennsylvania
West Virginia Network for Educational Telecomputing
Western Washington University
Wichita State University
Williams College
Worcester Polytechnic Institute
Wright State University

Xavier University

Yale University
Youngstown State University

==Phrack Inc.==

Volume Two, Issue 23, File 7 of 12

UTOPIA Index File 2

BITNET Member Institutions

December 1988

AK University of Alaska

AL Auburn University
Samford University
University of Alabama
University of Alabama at Birmingham
University of South Alabama

AR University of Arkansas
University of Arkansas at Little Rock
University of Arkansas for Medical Sciences

AZ Arizona State University
Maricopa County Community College District
Northern Arizona University
University of Arizona

CA California Institute of Technology
California Polytechnic State University-San Luis Obispo
California State University
Claremont Graduate School
Electric Power Research Institute
Harvey Mudd College
IBM Almaden Research Center
Lawrence Berkeley Laboratory
Naval Postgraduate School
Pepperdine University
Pomona College
Research Libraries Group
Salk Institute
San Diego Supercomputer Center
Santa Clara University
Stanford Linear Accelerator Center
Stanford Synchrotron Radiation Laboratory
Stanford University
University of California
University of California Berkeley
University of California Davis
University of California Irvine
University of California Los Angeles
University of California Riverside
University of California San Diego
University of California San Francisco
University of California Santa Barbara
University of California Santa Cruz
University of Southern California

CO Colorado School of Mines
Colorado State University
National Center for Atmospheric Research
University of Colorado at Boulder
University of Colorado at Colorado Springs
University of Colorado at Denver
University of Colorado Health Sciences Center
University of Denver

CT	Connecticut College
	Connecticut State University System
	Trinity College
	University of Connecticut
	University of Hartford
	Wesleyan University
	Yale University
DC	American University
	Catholic University of America
	Food and Drug Administration
	Gallaudet University
	George Washington University
	Georgetown University
	Georgetown University Medical Center
	Howard University
	National Academy of Sciences
	National Science Foundation
	Smithsonian Institution
	The World Bank
	University of the District of Columbia
DE	University of Delaware
FL	Florida Central Regional Data Center
	Florida Northeast Regional Data Center
	Florida State University
	Southeast Regional Data Center/FIU
	University of Central Florida
	University of Florida
	University of North Florida
	University of West Florida
GA	Emory University
	Georgia Institute of Technology
	Georgia State University
	University of Georgia Athens
HI	The Center for Cultural & Tech Exchange Btwn East and West
	University of Hawaii
IA	Drake University
	Grinnell College
	Iowa State University
	University of Iowa
ID	Boise State University
	University of Idaho
IL	Argonne National Laboratory
	College of DuPage
	De Paul University
	Educational Computing Network of Illinois
	Fermi National Accelerator Laboratory
	Illinois Institute of Technology
	Loyola University of Chicago
	Northern Illinois University
	Northwestern University
	Southern Illinois University
	Southern Illinois University at Edwardsville
	University of Chicago
	University of Illinois at Urbana-Champaign
	University of Illinois Chicago
IN	Ball State University
	Indiana State University
	Indiana University
	Indiana University/Purdue University at Indianapolis
	Purdue University

Rose-Hulman Institute of Technology
University of Notre Dame
Valparaiso University

KS Kansas State University
University of Kansas
University of Kansas Medical Center
Wichita State University

KY Transylvania University
University of Kentucky
University of Louisville

LA Louisiana State University
Louisiana State University Medical Center
Tulane University
University of New Orleans

MA Amherst College
Babson College
Bentley College
Boston College
Boston University
Brandeis University
Clark University
College of the Holy Cross
Hampshire College
Harvard University
IBM VNET Gateway
Massachusetts Institute of Technology
Mount Holyoke College
Northeastern University
Regents Computer Network
Smith College
Southeastern Massachusetts University
Tufts University
University of Massachusetts at Amherst
University of Massachusetts at Boston
Williams College
Worcester Polytechnic Institute

MD American Assoc of State Colleges Univs (AASCU) Meeting
Biotechnology Research Center
Catonsville Community College
Johns Hopkins University
Loyola College
Montgomery College
National Aeronautics and Space Administration
National Bureau of Standards
National Institutes of Health
Naval Health Sciences Education and Training Command
Space Telescope Science Institute
Towson State University
Uniformed Services University of the Health Sciences
University of Maryland

ME Bowdoin College
The Jackson Laboratory
University of Maine

MI Albion College
Central Michigan University
Macomb Community College
Merit Computer Network
Michigan State University
Michigan Technological University
Oakland Community College
University of Michigan
Wayne State University

MN Control Data Corporation
Gustavus Adolphus College
Macalester College
State University System of Minnesota System Office
University of Minnesota
University of Minnesota at Morris
University of Minnesota Duluth

MO Northeast Missouri State University
Saint Louis University
Southwest Missouri State University
University of Missouri
Washington University

MS Mississippi State University
University of Mississippi
University of Southern Mississippi

MT Montana State University

NC Appalachian State University
Davidson College
Duke University
East Carolina University
National Institute of Environmental Health Sciences
North Carolina State University
Triangle Universities Computation Center
Triangle Universities Nuclear Laboratory
United States Environmental Protection Agency
University of North Carolina at Chapel Hill
University of North Carolina at Charlotte
University of North Carolina at Greensboro
University of North Carolina Gen Ad Cntrl Off Ed Comptng Srvs

ND North Dakota Higher Education Computer Network

NE University of Nebraska - Omaha
University of Nebraska Computer Services Network
University of Nebraska Lincoln
University of Nebraska Medical Center

NH Dartmouth College
University of New Hampshire

NJ BITNET Network Information Center
Drew University
Educational Testing Service
EDUCOM
Exxon Research and Engineering Company
Institute for Advanced Study
Jersey City State College
John Von Neumann Center
New Jersey Educational Computer Network
New Jersey Institute of Technology
Princeton University
Rutgers University
Saint Peter's College
Seton Hall University
Stevens Institute of Technology
Trenton State College
University of Medicine & Dentistry of New Jersey

NM Los Alamos National Laboratory
New Mexico State University
University of New Mexico

NV University of Nevada

NY American Institute of Physics
American Physical Society

Association for Computing Machinery
BITNET-Internet Gateway
Brookhaven National Laboratory
Canisius College
City University of New York CUNY
Clarkson University
Cold Spring Harbor Laboratory
Colgate University
Columbia University
Columbia University Teachers College
Cornell University
Fordham University
General Electric Corporate Research & Development
Hofstra University
IBM Watson Scientific Research Center Yorktown
Iona College
Ithaca College
Le Moyne College
Long Island University
Manhattan College
Marist College
NASA Goddard Institute for Space Studies
New York State College of Ceramics at Alfred University
New York University
Pace University Pleasantville-Briarcliff Campus
Polytechnic University
Pratt Institute
Rensselaer Polytechnic Institute
Rochester Institute of Technology
Rockefeller University
Skidmore College
St. Lawrence University
State University of New York Ag and Tech College at Canton
State University of New York Ag and Tech College at Farmingdale
State University of New York at Albany
State University of New York at Binghamton
State University of New York at Buffalo
State University of New York at Stony Brook
State University of New York Central Administration
State University of New York College at Brockport
State University of New York College at Buffalo
State University of New York College at Cortland
State University of New York College at Fredonia
State University of New York College at Geneseo
State University of New York College at New Paltz
State University of New York College at Old Westbury
State University of New York College at Oneonta
State University of New York College at Oswego
State University of New York College at Plattsburgh
State University of New York College at Potsdam
State University of New York College of Technology at Alfred
State University of New York College of Technology at Delhi
State U of New York Health Science Center at Brooklyn
Syracuse University
Union College
University of Rochester
Vassar College

OH Bowling Green State University
Case Western Reserve University
Chemical Abstracts Service
Cleveland State University
Denison University
John Carroll University
Kent State University
Medical College of Ohio
Miami University
Oberlin College
Ohio State University
Ohio University

Ohio Wesleyan University
Online Computer Library Center (OCLC)
University of Akron
University of Cincinnati
University of Dayton
University of Toledo
Wright State University
Xavier University
Youngstown State University

OK Oklahoma State University
University of Oklahoma Norman Campus
University of Tulsa

OR Lewis and Clark College
Oregon State University
Portland State University
Reed College
Shriners Hospital for Crippled Children
University of Oregon

PA Allegheny College
Annenberg Research Institute
Bryn Mawr College
Bucknell University
Carnegie Mellon University
Dickinson College
Drexel University
Franklin and Marshall College
Gettysburg College
Haverford College
Indiana University of Pennsylvania
Lafayette College
Lehigh University
Millersville University of Pennsylvania
Pennsylvania State University
Rohm and Haas Company
Swarthmore College
Temple University
University of Pennsylvania
University of Pittsburgh
University of Scranton
Villanova University
West Chester University of Pennsylvania

PR National Astronomy and Ionosphere Center
University of Puerto Rico

RI Brown University
University of Rhode Island

SC Clemson University
Medical University of South Carolina
The Citadel, The Military College of South Carolina
University of South Carolina

SD Dakota State College
South Dakota State University

TN East Tennessee State University
Oak Ridge National Laboratory
Rhodes College
Tennessee Technological University
University of Tennessee
University of Tennessee at Chattanooga
University of Tennessee at Knoxville
University of Tennessee at Memphis
Vanderbilt University

TX Abilene Christian University

Baylor University
Pan American University
Rice University
Saint Mary's University of San Antonio
Sam Houston State University
Southern Methodist University
Southwest Texas State University
Stephen F. Austin State University
Tarleton State University
Texas A&M University
Texas Christian University
Texas Tech University
Trinity University
University of Houston
University of Houston at Clear Lake
University of North Texas
University of Texas at Arlington
University of Texas at Austin
University of Texas at Dallas
University of Texas at El Paso
University of Texas at Houston
University of Texas at San Antonio
University of Texas Health Science Center at San Antonio
University of Texas Medical Branch at Galveston
University of Texas Southwestern Medical Center at Dallas
University of Texas System

UT Brigham Young University
University of Utah
Utah State University

VA College of William and Mary
Continuous Electron Beam Accelerator Facility
George Mason University
James Madison University
National Radio Astronomy Observatory
Old Dominion University
Radford University
United States Geological Survey
University of Richmond
University of Virginia
Virginia Commonwealth University
Virginia Community College System
Virginia Polytechnic Institute and State University

VT Middlebury College
Norwich University
Saint Michael's College
University of Vermont

WA Fred Hutchinson Cancer Research Center
Pacific Lutheran University
University of Washington
Washington State University
Western Washington University

WI Lawrence University
Marquette University
Medical College of Wisconsin
University of Wisconisn - La Crosse
University of Wisconsin - Oshkosh
University of Wisconsin - Stout
University of Wisconsin Eau Claire
University of Wisconsin Madison
University of Wisconsin Milwaukee

WV Marshall University
West Virginia Network for Educational Telecomputing

WY University of Wyoming

==Phrack Inc.==

Volume Two, Issue 23, File 8 of 12

Getting Serious About VMS Hacking

by VAXbusters International

January 1989

The VAX/VMS operating system is said to be one of the most secure systems currently available. It has been massively extended in the past to provide features which can help system managers getting their machines locked up to abusers and to trace back any attempts to indiscriminate system security. As such, it is not easy getting into VMS machines now without having insider information, and it's even harder to stay in.

The following article describes some of the internals which make up the VMS security features, and tries to give hints what to do to remain undiscovered. The reader should be familiar with the VMS system from the programmer's point of view.

Some of the things mentioned are closely related to the internal workings of the VAX/VMS operating system. All descriptions are held as general as possible. It is tried to point out where weak points in the system are located, not to give step-by-step instructions on how to hack VMS machines. The main reason for this is, that it is very hard to remain undiscovered in a VMS system without having good knowledge of the whole system. This knowledge is only aquirable by experience.

To use some of the techniques described herein, some literature is recommended:

> "The VAX Architecture Handbook," published by DEC. This book describes the VAX processor, it's instruction set and it's hardware. It is a good book to have on your desk, since it costs nothing (just go to your local DEC store and ask for it) and is only in paperback format.
>
> "MACRO and Instruction Set," part of the VMS documentation kit. This is needed only if you want to program bigger things in MACRO. It's recommended reading, but you don't need to have it on your own normally.
>
> "VAX/VMS Internals and Data Structures" by L.Kenah and S.Bate. This is the bible for VMS hackers. It describes the inner workings of the system as well as most of the data structures used within the kernel. The Version published always is one version number behind the current VMS release, but as the VAX architecture doesn't change, it is the best source on a description how the system works. After you've read and understood this book, the VAX won't look more mysterious than your C64. You can order this book from DEC, the order number for the V3.0 version of the book is EY-00014-DP. The major drawback is the price, which is around $70-$100.

A good source of information naturally is the source code of the VMS system. The easiest way to snoop around in it is to get the microfiche set, which is delivered by DEC to all bigger customers of the system. The major disadvantage is that you need a fiche reader to use it. The fiche is needed if modifications to the system code are intended, unless you plan to disassemble everything you need. The VMS system is written in BLISS-32 and FORTRAN. BLISS is quite readable, but it might be worthwhile having a FORTRAN hacker around if you intend to do patch any of the programs implemented in FORTRAN. The source fiche always contains the current release, so it's useful to check if the information in "Internals and Data Structures" is still valid.

Hacker's Tools

There are several programs which are useful when snooping around on a VMS

system.

The most important utility might be the System Dump Analyzer (SDA), which is started with the command ANALYZE/SYSTEM. Originally, SDA was developed to analyze system crash dumps, which are created every time the machine crashes in a 'controlled' manner (bugcheck or opcrash). SDA can also be used to analyze the running system, which is the more useful function. A process which wants to run SDA needs the CMKRNL privilege. With SDA, you can examine any process and find out about accessed files and devices, contents of virtual memory (like typeahead and recall buffers), process status and more. SDA is a watching tool, so you normally can't destroy anything with it.

Another helpful tool is the PATCH utility, called up by the command PATCH. As VMS is distributed in a binary-only fashion, system updates are normally distributed as patches to binaries. PATCHES can be entered as assembler statements directly. Combined with the source fiche, PATCH is a powerful tool for your modifications and improvements to the VMS operating system.

Privileges

To do interesting things on the VMS system, you normally need privileges. The following lists describes some of the privileges which are useful in the onliner's daily life.

CMKRNL
CMEXEC These two privileges enable a user to execute arbitrary routines with KERNEL and EXECUTIVE access mode. These privileges are needed when one plans to access kernel data structures directly. CMKRNL is the most powerful privilege available, everything which is protected can be accessed utilizing it.

SYSPRV A process which holds this privilege can access objects via the system protection. A process holding the this privilege has the same access rights as a process running under a system UIC.

SHARE This allows a process to assign channels to nonshareable devices which already have channels assigned to them. This can be used to prevent terminal hangups and to assign channels to system mailboxes.

Process States And The Process Control Block

When you get into kernel hacking, you should pay special attention to the field PCB$L_STS. This field tells about the process status. Interesting bits are PCBV_DELPEN, PCBV_NOACNT and PCB$V_BATCH. There can be achieved astonishing effects by setting these bits.

Hideout

A nice possibility to have is to be unseen by a system manager. There are many ways to get invisible to SHOW USERS, but hiding from SHOW SYSTEM is another story, as it doesn't even use standard system calls to get a list of the currently running processes. And in fact, hiding from SDA is even harder, since it directly peeks kernel data structures. Anyway, being invisible to SHOW USERS is useful on small systems, where one user more could ring the alarm bell of the system operator.

One possibility to do this is to become a subprocess of some non-interactive job (like a BATCH or NETWORK process). The other way is to patch the PCB to become a BATCH process or to delete the terminal name (which makes SHOW USERS think you are non-interactive as well). Patching the PCB has a disadvantage: The system global variable SYS$GW_IJOBCNT which contains the number of interactive users must be directly decremented before you hide, and MUST be incremented before you log out.

If you forget this, the interactive job count will be wrong. If it becomes negative, strange effects will show up, which will confuse every system manager.

Accounting And Audits

The most nasty thing about VMS since release 4.2 is the security auditing feature. It enables the system manager to log almost every security relevant event he desires. For example, access to files, login failures and modification user authorization data base can all be monitored, logged and written to the system printer. The first thing to find out in a new, unknown system is the awareness of the system management. The status of the accounting system is easily determinable by the command SHOW ACCOUNTING. Normally, everything except IMAGE accounting is enabled. When IMAGE accounting is also enabled, this is the first hint to be careful. The second thing to check out is the status of the security auditing system. You need the SECURITY privilege to execute the command SHOW AUDIT.

If no audits are enabled, and image accounting is not turned on, the system normally is not set up to be especially secure. Such systems are the right playground for a system hacker, since one doesn't have to be as careful as one has to be on a correctly managed system.

Accounting

The main intention for running accounting on a system is the need to charge users for resources (cpu time, printer usage etc.) they use on the machine. On the other hand, accounting can be very useful to track down invaders. Luckily, accounting information is being logged in the normal file system, and as such one can edit out information which isn't supposed to be seen by sneaky eyes. The most important utility to handle accounting files is, naturally, the ACCOUNTING utility. It has options to collect information which is stored in accounting files, print it in a human readable manner, and, most importantly, edit accounting files. That is, you can edit all information out of an accounting file which you don't want to appear in reports anymore. The important qualifier to the ACCOUNTING command is /BINARY.

File Access Dates

One way for system managers to discover unwanted guests is to look out for modified system files. Fortunately, there are ways to modify the modification dates in a file's header. This can be done with RMS system calls, but there is no easy way to do that with pure DCL. There are several utilities to do this kind of things in the public domain, so look out in the DECUS catalog.

OPCOM

OPCOM is a process which logs system and security relevant events (like tape and disk mount transactions, security auditing messages etc.). OPCOM receives messages via a mailbox device, formats them, logs the event in the operator logfile (SYS$MANAGER:OPERATOR.LOG) and notifies all operators. Additionally, it sends all messages to it's standard output, which normally is the system console device _OPA0:. When OPCOM is started, one message is sent to the standard output announcing that the operator logfile has been initialized. Thus, it's not recommended to kill OPCOM to remain undiscovered, since the system manager most likely will get suspicious if the operator logfile has been initialized without an obvious reason. The elegant solution to suspend OPCOM, for the time where no operator messages shall come through. While OPCOM is suspended, all messages will be buffered in the mailbox device, where every process with sufficient privilege can read them out, thus avoiding that OPCOM reads those messages after it is restarted.

There is one problem with this solution though: OPCOM always has a read pending on that mailbox, and this read will be there even if the OPCOM process is suspended. Unless you're heavily into kernel hacking, there is no way to get rid of this read request. As such, the easy solution is to generate an unsuspicious operator message as soon as OPCOM is suspended. Afterwards, your own process (which can be a DCL procedure) reads all subsequent messages off the OPCOM mailbox until you feel save enough to have OPCOM resume it's work. By

the way, the OPCOM message mailbox is temporary and has no logical name assigned to it. You'll need SDA to get information about the device name.

Command Procedures

Timely, you'll need DCL procedures to have some routine work done automatically. It is important not to have strange command procedures lying around on a foreign system, since they can be easily read by system managers. Fortunately, a command file may be deleted while someone is executing it. It is good practice to do so, utilizing the lexical function F$ENVIRONMENT. If you need access to the command file itself from the running procedure, just assign a channel to it with OPEN.

Piggy-Backing

It's not normally a good idea to add new, possibly privileged accounts to a foreign system. The better approach is to to use accounts which have been unused for some months and to hide privileged programs or piggybacks which gain privilege to the caller by some mechanism. A piggyback is a piece of code which is added to a privileged system program, and which gives privileges and/or special capabilities to callers which have some kind of speciality (like a special process name, for example). Be careful not to change file sizes and dates, since this makes people suspicious.

Conclusion

This file just tries to give an impression how interesting VMS kernel hacking can be, and what possibilities there are. It of course is not complete, and many details have been left out. Hopefully, it has been useful and/or interesting lecture.

==Phrack Inc.==

Volume Two, Issue 23, File 9 of 12

Can You Find Out If Your Telephone Is Tapped?

by Fred P. Graham

"It Depends On Who You Ask"

Transcribed by VaxCat

December 30, 1988

Unlike most Americans, who suspect it, Sarah Bartlett at least knows she was overheard by an F.B.I. wiretap in the computer room of the Internal Revenue Service Building in Washington, across the street from the Justice Department. On April 25, as she sat at her card-punch machine, the postman handed her a registered letter containing a document known in police circles as a "wiretap notice." It told her that the Government had been given permission to intercept wire communications "to and from" two Washington telephones for a period of fifteen days after January 13, and that during this period her own voice had been heard talking to the parties on those phones. Miss Bartlett said nothing to the other girls in the computer room, but she must have been stunned. A few weeks later, federal agents came to the computer room and took her away, to face a variety of charges that amounted to being a runner for a numbers game.

There are no figures to disclose how many Americans have received such wiretap messages, and few people who have gotten them have spoken out. But the number could be over 50,000 by now. When Congress enacted the requirement in 1968 that notice of wiretap be given, it intended to sweep away the growing sense of national paranoia about electronic snoopery. But there seems to be an unabated national suspicion that almost everybody who is anybody is being tapped or bugged by somebody else. Herman Schwartz, a Buffalo, New York, law professor who is the American Civil Liberties Union's expert on Governmental eavesdropping, estimates that since 1968 between 150,000 and 250,000 Americans have been overheard by the Big Ear of the Federal Government or local police. "If you have anything to do with gambling or drugs, or if you're a public official involved in any hanky-panky and if you're a Democrat, or if you or your friends are involved in radical politics or black activism, you've probably been bugged," Professor Schwartz says.

Henry Kissinger wisecracks to friends that he won't have to write his memoirs, he'll just publish the F.B.I.'s transcripts of his telephone calls. Richard G. Kleindienst has had his Justice Department office "swept." Secretary of State William P. Rogers once shied away from discussing China policy over a liberal newspaper columnist's line. High-ranking officials in New York, Washington and Albany have been notified by the New York District Attorney's office that they may become targets of blackmailers because their visits to a swanky Manhattan whorehouse were recorded on hidden bugs. The technician who regularly sweeps the office of Maryland Governor Marvin Mandel, checking the Civil Defense hot-line telephone he had been instructed not to touch, recently found it was wired to bug the room while resting on the hook. Democratic officials waxed indignant over the five characters with Republican connections who were caught attempting to bug the Democratic National Committee headquarters in the Watergate hotel, but when they had earlier found less conclusive proof of the same kind of activity, they let it pass without public comment. The Omnibus Crime Control Act of 1968 makes it a crime, punishable by five years in jail and a $10,000 fine, to eavesdrop on a telephone call or a private conversation without a court order. Only federal law-enforcement officials and local prosecutors in states that have adopted similar wiretap legislation can get court permission to wiretap, and the law requires that within ninety days after a listening device is unplugged, wiretap notices must be sent to everyone whose phones or premises were bugged, plus anyone else (like Sarah Bartlett) who was overheard and might later be prosecuted because of it.

However, because of some private investigators and snoopy individuals nobody knows how many are ignoring the law against eavesdropping and getting away with it, and because none of the rules governing court-approved wiretapping in ordinary criminal investigations applies to the Federal Government's warrantless wiretapping in the name of "national security," no one can be certain his phone is safe. Before the Supreme Court ruled, 8 to 0, last June that the Government must get warrants for its wiretapping of domestic radicals in national-security cases, the F.B.I. wiretapped both homegrown and foreign "subversives" without court orders. The best estimates were that this accounted for between 54,000 and 162,000 of the 150,000 to 250,000 people who were overheard since 1968.

With warrantless wiretapping of domestic radicals now outlawed, the number of persons overheard on warrantless devices is expected to be reduced by about one fourth. But even with the courts requiring that more Government bugging be reported to the victims, paranoia is fed by improved technology. Bugging has now developed to the point that it is extremely difficult to detect, and even harder to trace to the eavesdropper. The hottest item these days is the telephone "hook-switch bypass," which circumvents the cutoff switch on a phone and turns it into a sensitive bug, soaking up all the sounds in the room while the telephone is sitting on its cradle. In its most simple form, a little colored wire is added to the jumble of wires inside a telephone and it is about as easy to detect as an additional strand in a plate of spaghetti. Even if it is found, the eavesdropper probably won't be. A check of the telephone line would most likely turn up a tiny transmitter in a terminal box elsewhere in the building or somewhere down the street on a pole. This would probably be broadcasting to a voice-activated tape recorder locked in the trunk of a car parked somewhere in the neighborhood. It would be impossible to tell which one it was.

My wife happened to learn about this at the time last year when The New York Times locked horns with the Justice Department over the Pentagon Papers, and I was covering the story for The Times. She became convinced that John Mitchell would stop at nothing and that the telephone in our bedroom was hot as a poker. After that, whenever a wifely chewing-out or amorous doings were brewing, I was always forewarned. If anything was about to happen in the bedroom too sensitive for the outside world to hear, my wife would first rise from the bed, cross the room, and ceremoniously unplug the telephone. "When someone finds out somebody else learned something they didn't want them to know, they usually jump to the conclusion they've been bugged," says Allan D. Bell Jr., president of Dektor Counterintelligence and Security Inc., in Springfield, Virginia, outside Washington. "If they thought about it, there was probably some other, easier way it got out."

Bell's point is that most people get information in the easiest, cheapest and most legal way, and that the person whose secrets have been compromised should consider first if he's thrown away carbons, left his files unlocked, hired a secretary who could be bribed, or just talked too much. There's an important exception, however, that many people don't know about. A party to a conversation can secretly record it, without violating any law. A person on one end of a telephone call can quietly record the conversation (the old legal requirement of a periodic warning beep is gone). Also, one party to a face-to-face conversation can secret a hidden recorder in his clothing. James R. Robinson, the Justice Department lawyer in charge of prosecuting those who get caught violating the anti-bugging law, insists that it is relatively rarely broken. He debunks the notion that most private eavesdropping is done in the executive suites of big business. Sex, not corporate intrigue, is behind ninety percent of the complaints he gets. After giving the snoopy spouse or lover a good scare, the Government doesn't even bother to prosecute do-it-yourself wiretappers. If a private investigator did the bugging, they throw the book at him.

Cost is the reason why experts insist there's less wiretapping than most people think. Private investigators who use electronic surveillance don't quote their prices these days, but people in the de-bugging business say the cost can range from $10,000 per month for a first-rate industrial job to $150 per day for the average private detective.

High costs also limit Government wiretapping. Last year the average F.B.I. tap

cost $600 per day, including installing the device, leasing telephone lines to connect the bugs to F.B.I. offices, monitoring the conversations and typing the transcripts. Considering the informative quality of most persons' conversations, it isn't worth it. Court records of the F.B.I.'s surveillances have demonstrated that when unguarded conversations are recorded, the result is most likely to be a transcript that is uninformative, inane or incomprehensible.

The folklore of what to do to thwart electronic surveillance is almost uniformly misguided or wrong. Robert F. Kennedy, when he was Senator, was said to have startled a visitor by springing into the air and banging his heels down onto his office floor. He explained this was to jar loose any bug J. Edgar Hoover might have planted. Whether he was teasing or not, experts say it wouldn't have done anything except bruise Senator Kennedy's heels. Former Senator Ralph Yarborough of Texas used to complain that, as each election season approached, the reception in his office phone would fade as the current was sapped by the multiple wiretaps installed by his political enemies. Those people who think poor reception and clicking on the line are due to wiretapping are giving wiretappers less credit and AT&T more, than either deserves. Present-day wiretaps are frequently powered by their own batteries, or they drain so little current that the larger normal power fluctuations make them undetectable, even with sensitive current meters.

Clicks on the line can be caused by loose connections in the phone, cables, or central office equipment, wet cables, defective switches in the central office, and power surges when batteries in the central office are charged. A sophisticated wiretap records conversations on a machine that turns itself silently on and off as you speak. The tap is designed to work without extraneous noises; your telephone isn't. If things you say in private or on the telephone seem to be coming back to you from unlikely sources, your first step should be to make a careful check of the room or rooms that might be bugged.

If the Federal Government is doing the eavesdropping, neither you nor any but the most experienced antibugging experts will detect it. Nobody has discovered a Justice Department wiretap for years, because the telephone company itself often taps the line and connects it to an FBI listening post. FBI bugs have become so sophisticated that the normal sweep techniques won't detect them, either. But the kind of eavesdropping that is being done by many private investigators is often so crude that even another amateur can find it. Room bugs come in two types: tiny microphones that send their interceptions to the outside by wire, and little radio transmitters that radio their overhearings to the outside.

Both are likely to be installed in electrical fixtures, because their power can be borrowed, their wires can be used to transmit the conversations to the listening post, and the fixtures' electrical innards serve as camouflage for the electric bugs. Your telephone has all these attributes, plus three built-in amplifiers the eavesdropper can borrow. You should first remove the plastic cover from your telephone's body and check inside for a wire of odd size or shape that seems to cut across the normal flow of the circuits. A bug or radio transmitter that feeds on your telephone's power and amplifiers will be a thimble-sized cylinder or cube, usually encased in black epoxy and wired into the circuit terminals.

Also check for the same devices along the telephone lines in the room or in the jack or box where the phone is attached to the baseboard. You should also unscrew the mouthpiece and earpiece to check for suspicious wires or objects. Even an expert would not detect a new item that's being sold illegally, a bugged mouthpiece that looks just like the one now in your telephone, and which can be switched with yours in a few seconds. After the phone check, look for suspicious little black forms wired into television sets, radios, lamps and clocks.

Also check heating and air-conditioning ducts for mikes with wires running back into the ducts. Radio transmitter bugs that have their own batteries can be quickly installed, but they can also be easier to find. Check under tables and chairs, and between sofa cushions. Remember they need to be near the point of likely conversations to assure good reception. Sometimes radio bugs are so cleverly concealed they are almost impossible to detect. A German manufacturer

advertises bugged fountain pens that actually write, table cigarette lighters that actually light, and briefcases that actually carry briefs.

Noting that the owner of such items can absent himself from delicate negotiations and leave his electronic ear behind, the company observes that "obviously, a microphone of this type opens untold opportunities during conferences, negotiations, talks, etc." If you suspect that your telephone has been tapped and your own visual inspection shows nothing, you can request the telephone company to check the line. The American Telephone and Telegraph Company estimates it gets about ten thousand requests from customers per year to check out their lines. These checks, plus routine repair service, turn up evidence of about two hundred fifty listening devices each year. When evidence of a tap is found, the company checks with the FBI and with local police in states where the laws permit police wiretapping with court orders. Until recently, if the tap was a court-approved job, the subscriber was assured that "no illegal device" was on the line. This proved so unsettling to the persons who requested the checks that now the telephone company says it tells all subscribers about any taps found. If this includes premature tidings of a court-approved FBI tap, that's a hassle that AT&T is content to leave to the Government and its suspect.

For those who have done the above and are still suspicious, the next step up in defensive measures is to employ an expert to de-bug your premises. A thorough job involves a minute inspection of the premises, including X-ray pictures of desk ornaments and other items that might contain hidden radio transmitters, the use of metal detectors to search out hidden microphones, checks of the electrical wiring for signs of unusual currents, and the use of a sensitive radio-wave detector to find any stray transmissions that a hidden bug might be giving out, plus employment of a radio field-strength meter to locate the bug.

With so much expertise required to do a sound detection job, and with no licensing requirements in most states to bar anybody from clapping on earphones and proclaiming himself an expert de-bugger, it is not surprising that the field abounds with quacks. A Pennsylvania construction company that had lost a series of close bids hired a local private detective last year to sweep its boardroom for bugs. The company's security chief, taking a dim view of the outside hotshot, took an ordinary walkie-talkie, taped its on-button down for steady transmission, and hid it behind the books on a shelf. He sat in a room down the hall and listened as the detective clumped into the room, swept around with his electronic devices, and pronounced the room clean.

Sometimes bogus de-buggers will give clients something extra for their money by planting a device and finding it during their sweep. One "expert" tried this twice in Las Vegas with organized-crime figures, who later compared notes and concluded they'd been taken. "Boy, was he sorry," chortled the Justice Department attorney who related the story. If you nevertheless want to have your place swept, things are complicated by the telephone company's ban on advertising by de-buggers.

As the Missouri Public Service Commission put it when it upheld the telephone company's refusal to include "de-bugging" in a detective's yellow-page ad, "advertising the ability to detect and remove electrical devices was, in fact, also advertising the ability to place those same devices. Anyone can be pretty certain of a reliable job by trying one of the major national detective agencies, Burns, Pinkerton or Wackenhut. They charge $40 to $60 per man-hour, for a job that will probably take two men a half day at least. They specialize in industrial work and shy away from domestic-relations matters. So if that's your problem, ask a lawyer or police official which private investigator in town is the most reliable de-bugger around.

It may seem too obvious to bear mentioning, but don't discuss your suspicions about eavesdropping in the presence of the suspected bug. W. R. Moseley, director of the Burns agency's investigations operations, say in probably a majority of the cases, a bugging victim tips off the eavesdropper that he's going to call in a de-bugger, thus giving the eavesdropper an opportunity to cover his tracks.

For the person who wants to have as much privacy as money can buy, the Dektor company is marketing a console about the size of a Manhattan telephone book which, for only $3,500, you can purchase to sit on your office desk and run a

constant check on the various things that might be done to your telephone and electric lines to overhear your conversations. It will block out any effort to turn your phone into a bug, will detect any harmonica bug, smother out any telephone tap using a transmitter to broadcast overheard conversations, detect any use of the electric lines for bugging purposes, and give off a frantic beep-beep! if anyone picks up an extension phone.

As sophisticated as this device is, there is one thing its promoters won't say it will do, detect a wiretap by the FBI. With the connection made in a place where no de-bugger will be allowed to check, and the G-men monitoring it on equipment no meter will detect, you can simply never know if the Government is listening. So if you're a businessman and think you're bugged by competitors, you're probably wrong. If you're a spouse or lover whose amours have gone public, the listening device can be found but probably nothing will be done about it. And if you're being listened to by the Biggest Ear of all, the Government, you'll never really know until you get your "wiretap notice."

VaxCat
