==Phrack Inc.==

Volume Four, Issue Thirty-Eight, File 1 of 15

Issue XXXVIII Index

P H R A C K 3 8

April 26, 1992

"Countdown to SummerCon '92"

"Get ready for the biggest and best computer
hacker PARTY conference of the year!"

Phrack Inc. is proud to be the official sponsor of the 6th Annual SummerCon, but this year is something different.

The date and location for this year's Summer Conference are for those with a need to know. SummerCon is a private party, its for our friends, and its our business and nobody elses'. Events from our past have made it necessary to keep the important specifics under wraps, so our theme this year is privacy.

Would be informants, ignorant and biased security professionals, and little malicious rodent hackers can forget about receiving an invitation. We are making a list and checking it twice. If you would like to receive an invitation and details about SummerCon then send mail to "summer@stormking.com".

Meanwhile, back at Phrack...

It appears that Phrack is getting VERY popular. At last count we had well over 775 people directly subscribed to the Phrack Mailing List. However, some people aren't overjoyed at Phrack's popularity. In recent postings to EFF newsgroups, complaints have been lodged that people downloading Phrack from "ftp.eff.org" account for more than 1/3 of all ftp traffic on that site. Some people at EFF have even suggested that Phrack be removed completely from their system. When the high and mighty defenders of Knight Lightning's First Amendment rights begin to balk, what does that say to the community at large about EFF and their agenda?

In this issue of Phrack we feature "Cellular Telephony" by Brian Oblivion! Brian tells us to expect more files on this topic from him in the near future, but for now we can start with this very substantial taste. Additionally, this issue will wrap up Black Kat's 3-part series on VAX/VMS and Dispater's 2-part defense manual for police radar. Rambone is back with his second file on the Pirate community and Datastream Cowboy picks up where Taran King left off in Phrack 30 with Network Miscellany. And if that wasn't enough, Mycroft brings us a file on Wide Area Information Services (WAIS). Subtitled "How Do I Use It and Why Should I Care?" It tells you about the service in general and gives directions for using WAIS to review Phrack.

Another spotlight file in this issue is "Standing Up To Fight The Bells." Knight Lightning brings forth a message and a warning about what is happening right now in the Congress and Senate of the United States, where the Bell Operating Companies are seeking to hold on to yet another monopoly to control. Be prepared to act and act fast or live forever with the consequences -- the future of information services controlled by Ma Bell.

And finally the full details of Computers, Freedom, & Privacy II appear both in a special file by Max Nomad and in two smaller articles in Phrack World News (part 3).

We're back and we're Phrack. Enjoy reading it because we enjoy writing it!

Chief Editor: Dispater (dispater@stormking.com)
Staff: Datastream Cowboy
Digital Disciple

NetLink
Takkel Genius
The Public

- -

Table Of Contents
~~~~~~~~~~~~~~~~~

~~~~~~~~~~~~~~~~~

==Phrack Inc.==

Volume Four, Issue Thirty-Eight, File 10 of 15

Standing Up To Fight The Bells

by Knight Lightning
kl@stormking.com

Did you hear about 1-800-54-Privacy? Did you decide to call? I did and the following is the information I received a few weeks later. It outlines some of the serious ramifications of what is going to happen if we do not actively support Congressional bills S 2112 and HR 3515.

The information comes from the American Newspaper Publisher's Association (ANPA). Keep in mind, they have a vested financial interest in information services as do many others, and in many ways, the newspaper industry can be and has been just as bad as the Regional Bell Operating Companies. However, in this particular situation, the ANPA has the right idea and does a pretty good job in explaining why we need to act now and act fast.

You know who I am, and what I've been through. My experiences have given me a unique perspective and insight into the methods and goals of the Regional Bell Operating Companies. They are inherently deceptive and if given even the slightest chance, they will screw the consumer and engage in anti-competitive market practices. Additionally, their tactics threaten our personal privacy as well.

The RBOCs must be stopped before it's too late.

:Knight Lightning

- -

1-800-54-Privacy
444 N. Michigan Avenue
Suite 900
Chicago, Illinois 60611

February 14, 1992

Dear Consumer:

If you're like many people, you may have been hesitant about leaving your name and address on our 1-800-54-PRIVACY phone line.

Why?

Quite simply, no one wants to give out information about themselves without knowing exactly how that information is going to be used.

But the truth is, you reveal information about yourself EACH AND EVERY TIME YOU PICK UP THE PHONE. By tracking who you call, how often you call and how long each conversation lasts, the seven regional Bell telephone companies have the capability to learn and know more about you than even the IRS.

In fact, with modern computer technology, there is practically no limit to what the Bells can learn about your personal life every time you pick up the phone. And there is virtually no limit -- only one's imagination -- to the ways they can take advantage of all the information they glean.

Of course its one thing to have the capability to do this snooping. It's another thing to have the incentive to actually do it.

Until October 7, 1991, the incentive just didn't exist for the Bells. Prior to

this date, the vast electronic networks of the Bell monopolies were just neutral carriers of phone messages, data, and other companies' fax, audiotex, and videotex services.

For example, when you last called a 1-900 or 1-800 line to get the latest stock quotes, sports scores, or headlines, your local phone company served simply as the pipeline for moving the billions of electrons in your call. The company that provided you with the information over the phone line was not -- and by law, could not be -- the phone company.

And that's the way things had been since 1984, when U.S. District Court Judge Harold Greene issued his now-famous decree breaking up the AT&T monopoly and spinning off control of local phone service to seven regional Bell companies.

In the decree, the Court expressly prohibited the individual Bells from entering three businesses -- cable TV, telephone manufacturing, and electronic information services.

Why?

After presiding over the lengthy AT&T anti-trust case and being exposed to hundreds upon hundreds of monopolistic abuses by AT&T, Judge Greene's Court was firmly convinced that, if allowed to enter any of these three current areas, the Bells would undoubtedly engage in the same monopolistic behavior that characterized their former parent.

In other words, while cutting off the hydra-like AT&T head, Judge Greene was fearful that, given too much leeway, AT&T's seven so-called "Baby Bell" off-spring might become equal or worse monsters themselves.

>From day one, however, the Bells undertook a long-term, multi-million dollar lobbying campaign to fight Judge Greene's ruling and try to convince the Justice Department, the higher courts, and even the U.S. Congress that they should be permitted to enter the content end of the information service business.

And, so, on October 7, 1991, after years of heavy lobbying, a higher court came through for the Bells and practically ordered Judge Greene to overturn his 1984 decree and open up the information services industry to the Bells.

In the 71-page ruling, a very reluctant Judge Greene devoted two-thirds of his decision to explaining why allowing the Bells to sell information services was bad for consumers and bad for America.

For example, he went to great length to discount the Bells' claim that, once given the green light, they would be better able to serve the public than the thousands of already existing electronic information services. To quote from his decision.

> "In the first place, the contention that it will take the Regional Companies (the Bells) to provide better information services to the American public can only be described as preposterous."

Judge Green also wrote:

> "Moreover, the Court considers the claim that the Regional Companies' entry into information services would usher in an era of sophisticated information services available to all as so much hype."

His decision also contains a warning regarding the prices consumers will be forced to pay for Bell-provided services:

> "The Regional Companies would be able to raise price by increasing their competitors' costs, and they could raise such costs by virtue of the dependence of their rivals' information services on local network access."

Finally, here's what Judge Greene had to say about his court's decision and the public good:

> "Were the Court free to exercise its own judgment, it would conclude

> without hesitation that removal of the information services restriction is incompatible with the decree and the public interest."

If Judge Greene's warnings as well as his profound reluctance to issue this ruling scare you, they should.

That's because the newly freed Bells now have the incentive, which they never had before, to engage in the anti-competitive, anti-consumer practices that Judge Greene feared.

Besides using your calling records to sell you information services they think you're predisposed to buy, the Bell's may well try to auction off your phone records to the highest bidder.

As a result, anyone who ever uses a phone could well be a potential victim of the Bell's abuse.

Consider the simple act of making a telephone call to an auto repair shop to schedule body work or a tune-up. By knowing that you made that call, your phone company might conclude that you're in the market for a new car and sell your name to local car dealers.

Another example. Think about calling a real estate broker for information on mortgage rates. Knowing you must be in the market for a house, the Bells could sell your name to other brokers. Or they could try to sell you their own electronic mortgage rate service.

Now let's say you and your spouse are having some problems and one of you calls a marriage counselor. Tipped off by information purchased from the phone company, a divorce lawyer shows up on your doorstep the next morning.

Finally, think about calling your favorite weather service hotline -- a competitor to the weather service operated by your local phone company. By keeping track of people who use its competitor's service, the phone company might just try to get you to buy its weather service instead.

Far-fetched? Not at all.

Nefarious? You bet.

That doesn't mean that, starting tomorrow, your phone company is going to start tracking who you call, how long your calls last, and who calls you. However, they could do it if they wanted to. And, based on past experience, some of them probably will do so at one point or another.

That's because the protest of gaining an unfair edge over the competition -- companies that have no choice but to depend upon the Bells' wires -- is just too tantalizing a temptation for the Bells to ignore.

As you might expect, the Bells claim that these fears are totally unfounded and that strict regulations are in place to prevent them from abusing your telephone privacy.

However, there simply aren't enough regulators in the world to control the monopolistic tendencies and practices of the Bells. Every single one of the seven Bells has already abused its position as a regulated monopoly. There is no reason to believe they won't in the future.

For example, the Georgia Public Service Commission recently found that BellSouth had abused its monopoly position in promoting its MemoryCall voice mail system. Apparently, operators would try to sell MemoryCall when customers called to arrange for hook-up to competitors' voice-mail services. Likewise, while on service calls, BellSouth repair personnel would try to sell MemoryCall to people using competitors' systems. BellSouth even used competitors' orders for network features as sales leads to steal customers.

In February 1991, US West admitted it had violated the law by providing prohibited information services, by designing and selling telecommunications equipment and by discriminating against a competitor. The Justice Department imposed a $10 million fine -- 10 times larger than the largest fine imposed in

any previous anti-trust division contempt case.

In February 1990, the Federal Communications Commission found that one of Nynex's subsidiaries systematically overcharged another Nynex company $118 million for goods and services and passed that extra cost on to ratepayers.

The abuses go on and on.

In this brave new world, however, it's just not consumers who will suffer. Besides invading your privacy, the Bells could abuse their position as monopolies to destroy the wide range of useful information services already available.

Right now, there are some 12,000 information services providing valuable news, information, and entertainment to millions of consumers. Every one of these services depends on lines owned and controlled by Bell monopolies.

This makes fair competition with the Bells impossible.

It would be like saying that Domino's Pizzas could only be delivered by Pizza Hut.

It would be like asking a rival to deliver a love note to your sweetheart.

It would be a disaster.

If the Bells aren't stopped, they will make it difficult -- if not impossible -- for competitors to use Bell wires to enter your home.

They could deny competitors the latest technological advances and delay the introduction of new features. They could even undercut competitor's prices by inflating local phone bills to finance the cost of their own new information services.

In the end, the Bells could drive other information services out of business, thereby dictating every bit of information you receive and depriving the American public out of the diversity of information sources it deserves and that our form of government demands.

Can something be done to stop the Bells?

Yes, absolutely.

You can take several immediate steps to register your views on this issue. Those steps are described in the attached "Action Guidelines" sheet. Please act right away.

In the meantime, on behalf of our growing coalition of consumer groups, information services providers, and newspapers, thank you for your interest in this important issue.

Sincerely,

Cathleen Black
President and Chief Executive Officer
American Newspaper Publishers Association

- -

ACTION GUIDELINES

Something is very wrong when a monopoly is put into the position where it can abuse your privacy, drive competitors from the market, and even force you, the captive telephone ratepayer, to subsidize the costs of new information services ventures.

Can something be done to stop this potential abuse?

Absolutely.

WHAT YOU CAN DO. The first step is to call or write your local telephone company to assert your right to privacy.

The second step is to write your U.S. Representative and U.S. Senators and urge them to support House bill 3515 and Senate bill 2112.

Since the purpose of both HR 3515 and S 2112 is to prevent the Bells from abusing their monopoly position, not to prevent legitimate competition, the Bells would be free to sell information services in any area of the country where they do not have a monopoly -- in other words, 6/7 of the country.

However, the bills would delay entry of the Bell companies into the information services industry in their own regions until they no longer held a monopoly over local phone service. As soon as consumers were offered a real choice in local phone service -- whether it be cellular phones, satellite communications, or other new technology -- the Bells would be free to offer any information services they wanted.

Both bills are fair to everyone. They protect consumer privacy and ensure that the thriving information services industry will remain competitive.

Quick action is need to pass these bills. A hand-written letter stating your views is the most effective way of reaching elected officials. It is proof positive that you are deeply concerned about the issue.

POINTS TO MAKE IN YOUR LETTER

You may wish to use some or all of the following points:

> A phone call should be a personal and private thing -- not a sales marketing tool for the phone company.
>
> The Bells should not be allowed to take unfair advantage of information they can obtain about you by virtue of owning and controlling the wires that come into homes.
>
> The Bells must not be allowed to abuse their position as monopolies to drive existing information services out of business.
>
> The Bells should not be permitted to engage in activities that would deprive Americans of the information diversity they deserve and that our form of government demands.
>
> The Bells should not be permitted to finance information services ventures by inflating the phone bills of captive telephone ratepayers.

AFTER YOU'VE WRITTEN YOUR LETTER

After you've written your letter or made your phone call, please send us a letter and tell us. By sending us your name and address, you'll receive occasional updates on the massive effort underway to prevent the Bells from invading your privacy and turning into the monopolistic monsters that Judge Greene warned about.

There's one more thing you can do. Please ask your friends, relatives, neighbors, and co-workers to urge their U.S. Representatives and Senators to support HR 3515 and S 2112. We need everyone's help if we're going to stop the Bells.

1-800-54-PRIVACY
444 N. Michigan Avenue
Suite #900
Chicago, Illinois 60611

* * * * * ** * * * * ** *

by Toby Nixon
tnixon@hayes.com

February 7, 1992

DISCLAIMER: The following is my personal position on this matter, and not necessarily that of my employer.

I am appalled at the RBOC's disinformation regarding HR 3515/S 2112, which propose to limit RBOC entry into information services until fair competition is possible. Every time one of the RBOC ads has played on the TV or radio, appeared in the newspaper, and now in the information they mailed to me, I can't help but stand up out of my chair and scream because of the contemptible lies.

Clearly, all of the services they claim are being held back are, or could be, available TODAY. We are IN the Information Age; where have they been? It's HERE, not "just over the horizon." We don't need the RBOCs to provide these services; all the RBOCs need to do is continue to provide the transmission services, which they do today. Unfortunately, the majority of the citizens of the USA don't know that these services are already available WITHOUT RBOC HELP -- and the RBOCs are taking advantage of this lack of knowledge to try to gain popular support for their positions.

What would happen if the RBOCs were to enter these markets? It is clear to me, based on their past performance in similar situations (such as voicemail) that they would leverage their monopoly on local telephone service to force competitors out of the market. They will use their guaranteed return on investment income from their monopoly on POTS to subsidize their information services (even providing co-location with central office switches is a subsidy), thereby indeed providing the "affordability" they talk about -- until the competition is driven out of the marketplace. Then the RBOCs will be free to raise the rates as high as they wish! With their monopoly on access, they could easily sabotage access to competitive services and make the RBOC services look better (just being co-located will provide better circuit quality and response times). While all of the competition would have to pay exorbitant rates for ONA services (to obtain ANI information, billing to phone accounts, etc.), the phone company has this free. Free competition? Hardly!

Many of you know that I am a Libertarian, and strongly oppose government regulation of business. The logical position for a Libertarian might appear to be to support the RBOC's fight against further regulation. But the fact is that they've enjoyed this GOVERNMENT-IMPOSED monopoly for decades; in too many ways, the RBOCs function as though they were an arm of the government. They have effectively no competition for local access. Every competitive service MUST use the RBOCs' facilities to reach their customers. This places the RBOCs in the position of being able to effectively control their competition -- meaning there would be no effective competition at all.

Despite their protestations that the proposed legislation would limit "consumer choice" and "competition", the reality is that provision of such services by RBOCs, so long as they remain the sole provider of local telephone service in most of the country, would be anti-choice and anti-competitive, plain and simple. It would be ABSOLUTELY UNFAIR for the government to turn them loose to use their monopoly-guaranteed income to try to put independent information services (even BBSes) out of business, when it is the government that has permitted (required!) them to get the monopoly in the first place.

It absolutely disgusts me that in their printed materials the RBOCs go so far as to forment class warfare. They talk about "the spectre of 'information rich' versus 'information poor'". They say that minorities, the aged, and the disabled support their position, to raise liberal guilt and stir up class envy (but without disclosing what have certainly been massive contributions to these groups in return for their support). They further stir up class envy by making the point that Prodigy and CompuServe customers are "... highly educated professionals with above average incomes, owning homes valued above national norms ... the world's most affluent, professional, and acquisitive people," as though this were somehow evil! They attack, without stating any evidence, the alleged "reality" that the only reason this legislation is proposed is to prop

up newspaper advertising revenues (the whole attitude of "evil profits" is so hypocritical coming from those for whom profits are guaranteed, and whom never mention the fact that they're not entering information services out of altruism but only because they seek to expand their own profits!). They invoke jingoistic fervor by talking about services "already being enjoyed by citizens of other countries" (but at what incredible cost?).

The materials are packed with this politically-charged rhetoric, but completely lacking in facts or reasonable explanation of the basis for the positions of either side. Their letter isn't written for a politically and technologically aware audience, but for those who are attuned to the anti-capitalistic culture of envy and redistribution. It isn't written for those trying to make an informed decision on the issues, but is intended simply to rally the ignorant into flooding Congressional offices with demands for services that most of the writers wouldn't know the first thing to do with, and which the writers don't realize are available without the RBOCs.

They talk about some supposed "right" of individuals to participate in "the Information Age", regardless of, among other things, INCOME. Does all of this appeal to the plight of the poor and disadvantaged mean that these services will be available regardless of ability to pay? Hardly! WE, the taxpayers, WE, the RBOC customers, without any choice of who provides our local phone service, will pay -- through the nose -- either in the form of cross-subsidization of "lifeline" (!) information services by those of us paying "full" residential rates or business rates, or by tax-funded government subsidies or credits going directly to the RBOCs. Does anybody really think that the RBOCs will cover the cost of providing these services to the "information poor" out of their profits? What a ridiculous idea!

The fact that the RBOC position is supported by groups like the NAACP and the National Council on Aging -- representing the most politically-favored, most tax-subsidized groups in America -- make it clear that they fully intend for the cost of such services to be born by the middle class and small business-people of America. Once again, the productive segments of society get screwed. Once again, private businesses which have fought to build themselves WITHOUT any government-granted monopoly will be forced out, to be replaced with politically-favored and politically-controllable socialized services. Once again, America edges closer to the fascist system which has been so soundly rejected elsewhere. When will we ever learn?

We SHOULD all write to our Congressmen and Senators. We should demand that they pass HR 3515 and S 2112, and keep them in force unless and until the RBOCs give up their local telephone monopolies and allow truly free competition -- which means long after the monopolies are broken up, until the lingering advantages of the monopoly are dissipated. Of course, the RBOCs could spin off entirely independent companies to provide information services -- with no common management and no favored treatment in data transmission over the other independent information services -- and I would cheer. But so long as they have a chokehold on the primary _delivery vehicle_ for information services in America, their protestations for "free competition" ring incredibly hollow.

Toby Nixon	Voice +1-404-840-9200	Telex 151243420
2595 Waterford Park Drive	Fax +1-404-447-0178	CIS 70271,404
Lawrenceville, Georgia 30244	BBS +1-404-446-6336	AT&T !tnixon
USA	Internet	tnixon@hayes.com

RHC Tactics Blamed For Failure Of Information Services Bill April 1, 1992

Taken from Communications Daily (Page 4)

Rep. Cooper (D-Tenn.) said that his legislation to put conditions on RHC provision of information services (HR-3515) didn't have much chance of success >from time bill was introduced. At panel discussion in Washington sponsored by National Press Forum, he said outlook for bill was "pretty grim," and that only hope for success would be if powerful committee chairman came to rescue. That's unlikely, he said.

Cooper said he has about 48 co-sponsors for bill and Senate version (S-2112)

has none. In strong attack on RHCs, he said RHCs were responsible for lack of support and said members of Congress were intimidated by ad campaign against sponsors and co-sponsors of HR-3515 -- what he termed "a $150,000 penalty" for sponsoring legislation. Cooper also criticized RHCs for sponsoring organizations without letting the public know of their interest, naming specifically Small Business for Advertising Choice, with headquarters in Washington. He said he didn't mind legitimate "grass-roots" campaigns, but objected to "Astroturf campaigns."

Disputes with RHCs broke into the open dramatically during Cooper's intense exchange with Southwestern Bell Vice-President Horace Wilkins, head of RHC's Washington office. Cooper said that if RHCs were truly interested in providing information services, they would push for sponsorship of amendment to cable reregulation legislation to allow telco entry. But Bells were "AWOL" on issue, Cooper said, even though there are members of House Telecom Subcommittee who would introduce such amendment if RHCs asked. Wilkins said one House chairman, whom he declined to name, had told RHCs not to participate by pushing telco entry amendment. Cooper responded: "Who told you?" He told Wilkins: "You have the opportunity of a lifetime."

Wilkins challenged Cooper: "Why don't you take the lead" and introduce amendment? Cooper replied he would do so if SWB would promise its support. Wilkins responded: "If it's the right thing, we'll be with you." Cooper replied that RHCs reportedly had been told not to push for such amendment, and neither he nor Wilkins would say which powerful House figure was against telco entry. Without RHC backing, any introduction of telco entry amendment "would have zero support," Cooper said. He said RHCs have backed away from active support of legislation to lift the MFJ manufacturing bar because they're afraid his measure might be attached to it. Wilkins disagreed, saying RHCs were backing the bill.

Mark MacCarthy, Cap/ABC vice-president, said the strongest argument against RHC entry into information services is that there's no evidence that "new and better information" would be provided to public. RHCs could provide more efficient network architectures and distribution, he said, but "not better programming." There's a historical example of "dark side of diversity" in which radio programmers once supported live symphony orchestras and provided quality content, MacCarthy said, but now, in an era in which there are many competitors, most stations obtain most of their programming free, on tape from record companies.

==Phrack Inc.==

Volume Four, Issue Thirty-Eight, File 11 of 15

The Digital Telephony Proposal

by the Federal Bureau of Investigation

Phone Tapping Plan Proposed March 6, 1992

By Associated Press

Law Enforcement Agencies Would Have Easier Access

WASHINGTON -- The Bush administration wants you to pay a little more for telephone service to make it easier for the FBI or local police to listen in on the conversations of suspected criminals.

The Justice Department is circulating a proposal in Congress that would force telephone companies to install state-of-the-art technology to accommodate official wiretaps. And it would authorize the Federal Communications Commission to grant telephone companies rate increases to defray the cost.

A copy of the legislation was obtained by The Associated Press.

Attorney General William Barr discussed the proposal last week with Senator Ernest Hollings, D-S.C., chairman of the Senate Commerce Committee, which oversees the FCC according to congressional sources who spoke on condition of anonymity.

Justice Department spokesman Paul McNulty refused to comment on the proposal.

The bill was drafted by the FBI and the Justice Department in response to dramatic changes in telephone technology that make it difficult for traditional wiretapping methods to pick up conversations between two parties on a telephone line.

The Justice Department's draft proposal states that the widespread use of digital transmission, fiber optics and other technologies "make it increasingly difficult for government agencies to implement lawful orders or authorizations to intercept communications in order to enforce the laws and protect the national security."

The FBI has already asked Congress for $26.6 million in its 1993 fiscal year budget to help finance a five-year research effort to help keep pace with the changes in telephone technology.

With the new technology that is being installed nationwide, police can no longer go to a telephone switching center and put wiretap equipment on designated lines.

The advent of so-called digital transmission means that conversations are broken into bits of information and sent over phone lines and put back together at the end of the wire.

The bill would give the FCC 180 days to devise rules and standards for telephone companies to give law enforcement agencies access to conversations for court-ordered wiretapping.

The attorney general would be empowered to require that part of the rulemaking proceedings would be closed to the public, to protect the security of eavesdropping techniques used by law enforcement.

Phone companies would have 180 days to make the necessary changes once the FCC issues the regulations.

The bill would prohibit telephone companies and private exchanges from using equipment that doesn't comply with the new FCC technology standards.

It would give the attorney general power to seek court injunctions against companies that violate the regulations and collect civil penalties of $10,000 a day.

It also would give the FCC the power to raise telephone rates under its jurisdiction to reimburse carriers. The FCC sets interstate long distance rates and a monthly end-user charge -- currently $2.50 -- that subscribers pay to be connected to the nationwide telephone network.

Telephone companies will want to examine the proposal to determine its impact on costs, security of phone lines and the 180-day deadline for implementing the changes, said James Sylvester, director of infrastructure and privacy for Bell Atlantic.

Though no cost estimates were made available, Sylvester estimated it could cost companies millions of dollars to make the required changes. But rate hikes for individual customers would probably be quite small, he said.

As Technology Makes Wiretaps More Difficult, F.B.I. Seeks Help March 8, 1992

By Anthony Ramirez (New York Times)(Page I12)

The Department of Justice says that advanced telephone equipment in wide use around the nation is making it difficult for law-enforcement agencies to wiretap the phone calls of suspected criminals.

The Government proposed legislation requiring the nation's telephone companies to give law-enforcement agencies technical help with their eavesdropping. Privacy advocates criticized the proposal as unclear and open to abuse.

In the past, the Federal Bureau of Investigation and other agencies could simply attach alligator clips and a wiretap device to the line hanging from a telephone pole. Law-enforcement agents could clearly hear the conversations. That is still true of telephone lines carrying analog transmissions, the electronic signals used by the first telephones in which sounds correspond proportionally to voltage.

But such telephone lines are being steadily replaced by high-speed, high-capacity lines using digital signals. On a digital line, F.B.I. agents would hear only computer code or perhaps nothing at all because some digital transmissions are over fiber-optic lines that convert the signals to pulses of light.

In addition, court-authorized wiretaps are narrowly written. They restrict the surveillance to particular parties and particular topics of conversation over a limited time on a specific telephone or group of telephones. That was relatively easy with analog signals. The F.B.I. either intercepted the call or had the phone company re-route it to an F.B.I. location, said William A. Bayse, the assistant director in the technical services division of the F.B.I.

But tapping a high-capacity line could allow access to thousands of conversations. Finding the conversation of suspected criminals, for example, in a complex "bit stream" would be impossible without the aid of phone company technicians.

There are at least 140 million telephone lines in the country and more than half are served in some way by digital equipment, according to the United States Telephone Association, a trade group. The major arteries and blood vessels of the telecommunications network are already digital. And the greatest part of the system, the capillaries of the network linking central telephone offices to residences and businesses, will be digital by the mid-1990s.

Thousand Wiretaps

The F.B.I. said there were 1,083 court-authorized wiretaps -- both new and continuing -- by Federal, state, and local law-enforcement authorities in 1990, the latest year for which data are available.

Janlori Goldman, director of the privacy and technology project for the American Civil Liberties Union, said she had been studying the development of the F.B.I. proposal for several months.

"We are not saying that this is not a problem that shouldn't be fixed," she said, "but we are concerned that the proposal may be overbroad and runs the risk that more information than is legally authorized will flow to the F.B.I.

In a news conference in Washington on Friday, the F.B.I. said it was seeking only to "preserve the status quo" with its proposal so that it could maintain the surveillance power authorized by a 1968 Federal law, the Omnibus Crime Control and Safe Streets Act. The proposal, which is lacking in many details is also designed to benefit state and local authorities.

Under the proposed law, the Federal Communications Commission would issue regulations to telephone companies like the GTE Corporation and the regional Bell telephone companies, requiring the "modification" of phone systems "if those systems impede the Government's ability to conduct lawful electronic surveillance."

In particular, the proposal mentions "providers of electronic communications services and private branch exchange operators," potentially meaning all residences and all businesses with telephone equipment.

Frocene Adams, a security official with US West in Denver is the chairman of Telecommunications Security Association, which served as the liaison between the industry and the F.B.I. "We don't know the extent of the changes required under the proposal," she said, but emphasized that no telephone company would do the actual wiretapping or other surveillance.

Computer software and some hardware might have to be changed, Ms. Adams said, but this could apply to new equipment and mean relatively few changes for old equipment.

FBI Wants To Ensure Wiretap Access In Digital Networks March 9, 1992

Taken from Communications Daily (Page 1)

Proposed legislation being floated by Justice Dept. and FBI would require RHCs and equipment manufacturers to reengineer their products so that federal, state and local law enforcement agencies could wiretap digital communications systems of all types, Bureau said. The proposal is a "collaborative effort" at "highest levels" involving law enforcement officials, government agencies, telephone executives and equipment manufacturers, said John Collingwood of FBI's office for legislative affairs. It seeks to authorize FCC to grant telcos rate increases to defray the cost of reengineering the network to bring it into compliance.

Associated Press reported Attorney General William Barr discussed the proposal last week with Sen. Hollings (D.-S.C.), chairman of Senate Commerce Committee; however, Committee staffers wouldn't comment. Sources at FCC said they hadn't heard of the proposal, and neither had several RHCs we contacted.

The bill was drafted by FBI and Department in response to what FBI Director William Sessions said were dramatic changes in telephone technology that have "outpaced" government ability to "technologically continue" its wiretapping activities. James Kallestrom, FBI's chief of technical services section, said the bill wouldn't extend the Bureau's "court-authorized" electronic surveillance authority, but would seek simply to maintain status quo with digital technology. New legislation is needed because law enforcement agencies no longer can go into a switching center and place a tap on single phone line, owing to complex digital multiplexing methods that often route number and voice signals over different channels. Kallestrom said digital encoding also doesn't allow specific wiretap procedures, unlike analog systems, which use wave forms. Bureau wants telephone companies and equipment manufacturers to "build in" the ability to "give us what we want." He said legislation wouldn't mandate how companies comply, only that they do. William Bayse, chief of FBI's Technical Services Division, said the reengineering process would be "highly complex" but could be done at the software level.

The FBI said it has been in contact with all telcos and "several" equipment manufacturers to get their input to determine feasibility. Bayse said FBI had done preliminary cost analysis and estimated changes would run into "tens of millions," declining to narrow its estimates further. The bill would give FCC the authority to allow RHCs to raise rates in order to make up the costs of implementing the new procedures. Although FBI didn't have any specifics as to how FCC would go about setting those rates, or whether state PUCs would be involved in the process, they speculated that consumer telephone rates wouldn't go up more than 20 cents per month.

The bill would give FCC 120 days to devise rules and standards for telcos to bring the public network into compliance. However, the Commission isn't a standards-making body. When questioned about the confusing role that the bill would assign to FCC, FBI's Collingwood said: "The FCC is the agency that deals with phone companies, so we put them in charge." He acknowledgedn that the bill "needs work" but said the FBI was "surprised" by the leak to press. However, he said that the language was in "very early stages" and that FBI wasn't averse to any changes that would bring swifter passage.

Other confusing aspects of proposal: (1) Short compliance time (120 days) seems to bypass FCC's traditional rulemaking procedures, in which the public is invited to submit comments; (2) No definition is given for "telecommunications equipment or technology;" (3) Provision that the attorney general direct that any FCC proceeding concerning "regulations, standards or registrations issued or to be issued" be closed to the public again would violate public comment procedures.

FBI said legislation is the "least costly alternative" in addressing the issue. It said software modifications in equipment now would save "millions of dollars" over making changes several years from now. However, the agency couldn't explain how software programming changes grew more expensive with time. FBI's Kallestrom said: "Changes made now can be implemented easier over time, rather than having to write massive software changes when the network gets much more complicated." FBI already has asked Congress for $26.6 million in its proposed 1993 budget to help finance a 5-year research effort to help keep pace with changes in telephone technology. Asked why that money couldn't be used to offset the price of government-mandated changes as the bill would require, FBI declined to comment, saying: "We may look at having government offset some of the cost as the bill is modified."

CPSR Letter on FBI Proposal March 9, 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~

By David Banisar (CPSR) <banisar@washofc.cpsr.org>

CPSR and several other organizations sent the following letter to Senator Patrick Leahy regarding the FBI's recent proposal to undertake wire surveillance in the digital network.

If you also believe that the FBI's proposal requires further study at a public hearing, contact Senator Hollings at the Senate Committee on Commerce. The phone number is (202)224-9340.

Dave Banisar,
CPSR Washington Office
==========

March 9, 1992

Chairman Patrick Leahy
Senate Subcommittee on Law and Technology
Committee on the Judiciary
United States Senate
Washington, DC 20510

Dear Senator Leahy,

We are writing to you to express our continuing interest in communications
~~~~~~~~~~~~~~~~~~~~~~~~~~

privacy and cryptography policy. We are associated with leading computer and telecommunication firms, privacy, civil liberties, and public interest organizations, as well as research institutions and universities. We share a common concern that all policies regarding communications privacy and cryptography should be discussed at a public hearing where interested parties are provided an opportunity to comment or to submit testimony.

Last year we wrote to you to express our opposition to a Justice Department sponsored provision in the Omnibus Crime Bill, S. 266, which would have encouraged telecommunications carriers to provide a decrypted version of privacy-enhanced communications. This provision would have encouraged the creation of "trap doors" in communication networks. It was our assessment that such a proposal would have undermined the security, reliability, and privacy of computer communications.

At that time, you had also convened a Task Force on Privacy and Technology which looked at a number of communication privacy issues including S. 266. The Task Force determined that it was necessary to develop a full record on the need for the proposal before the Senate acted on the resolution.

Thanks to your efforts, the proposal was withdrawn.

We also wish to express our appreciation for your decision to raise the issue of cryptography policy with Attorney General Barr at his confirmation hearing last year. We are pleased that the Attorney General agreed that such matters should properly be brought before your Subcommittee for consideration.

We write to you now to ask that you contact the Attorney General and seek assurance that no further action on that provision, or a similar proposal, will be undertaken until a public hearing is scheduled. We believe that it is important to notify the Attorney General at this point because of the current attempt by the administration to amend the Federal Communications Commission Reauthorization Act with provisions similar to those contained in S. 266.

We will be pleased to provide assistance to you and your staff.

Sincerely yours,

Marc Rotenberg,
Computer Professionals for Social Responsibility

David Peyton,
ITAA

Ira Rubenstein,
Microsoft

Jerry Berman,
Electronic Frontier Foundation

Michael Cavanaugh,
Electronic Mail Association

Martina Bradford,
AT&T

Evan Hendricks,
US Privacy Council

Professor Dorothy Denning,
Georgetown University

Professor Lance Hoffman,
George Washington University

Robert L. Park,
American Physical Society

Janlori Goldman,
American Civil Liberties Union

Whitfield Diffie,
Sun Microsystems

John Podesta,
Podesta and Associates

Kenneth Wasch,
Software Publishers Association

John Perry Barlow,
Contributing Editor, Communications of the ACM

David Johnson,
Wilmer, Cutler & Pickering

cc: Senator Joseph R. Biden, Jr
Senator Hank Brown
Senator Ernest F. Hollings
Senator Arlen Specter
Senator Strom Thurmond
Representative Don Edwards
Attorney General Barr
Chairman Sikes, FCC

FBI, Phone Firms in Tiff Over Turning on the Taps March 10, 1992

By John Mintz (Washington Post)(Page C1)

Technology Has Made Eavesdropping Harder

The FBI says technology is getting ahead of taps.

The bureau says the digital technology in new telephone networks is so complicated -- it translates voices into computerized blips, then retranslates them into voices at the other end -- that agents can't capture conversations.

So the FBI wants a law requiring phone companies to re-engineer their new phone networks so the taps work again.

But the phone companies warn that the proposal could raise ratepayers' monthly bills.

And civil liberties groups say the technological changes sought by the FBI could have an unintended effect, making it easier for criminals, computer hackers and even rogue phone company employees to tap into phone networks.

"We have grave concerns about these proposals," said Jim McGann, a spokesman for AT&T. "They would have the effect of retarding introduction of new services and would raise prices."

Bell Atlantic Corporation, owner of Chesapeake & Potomac Telephone Company here, said the changes could cost its own ratepayers as much as hundreds of millions of dollars.

The cause of the FBI's concern is a new generation of digital technologies in which phone conversations are translated into the computer language of zeroes and ones, then bundled with other conversations for speedy transmission, and finally retransformed into voices.

Another problem for the FBI is fiber-optic technology, in which conversations are changed into pulses of light zapped over hair-thin strands of glass. The U.S. government has delayed sales of fiber-optic equipment to the former Soviet Union because of the difficulty of tapping it.

The FBI proposed a law requiring phone companies to modify their networks to

make wiretaps easier. The agency would still have to obtain a court order to tap a line, as it does now. It also proposed allowing the Federal Communications Commission to let the phone companies pass the costs on to consumers and letting the FCC consider the issues in closed-door hearings to keep secret the details of phone system security.

"Without an ultimate solution, terrorists, violent criminals, kidnappers, drug cartels and other criminal organizations will be able to carry out their illegal activities using the telecommunications system without detection," FBI Director William S. Sessions said in a prepared statement. "This proposal is critical to the safety of the American people and to law enforcement officers."

In the past, investigators would get the phone company to make adjustments at switching facilities, or would place taps at junction boxes -- hard metal structures on concrete blocks in every neighborhood -- or even at telephone junction rooms in the basements of office and apartment buildings.

But sometimes tappers get only bursts of electronic blipping. The FBI said the new technologies have defeated wiretap attempts on occasion -- but it declined to provide details.

To get the blips retranslated back into conversation, tappers have to place their devices almost right outside the targeted home or office. Parking FBI trucks outside targets' houses "could put agents in danger, so it's not viable," said Bell Atlantic spokesman Kenneth A. Pitt.

"We don't feel our ratepayers should pay that money" to retool networks, said Bill McCloskey, spokesman for BellSouth Corporation, a major phone company based in Atlanta.

Since there are 150 million U.S. phone lines, a cost of $ 1 billion that's passed on to ratepayers could translate into about $ 6.60 per consumer, industry officials said.

Rather than charge ratepayers, Pitt said, the government should pay for the changes. Bell Atlantic prefers continued FBI and industry talks on the subject to a new law.

The FBI proposes that within 120 days of enactment of the law it seeks, the FCC would issue regulations requiring technological changes in the phone system and that the modifications be made 60 days after that. The FCC rarely moves on even the simplest matter in that time, and this could be one of the most complex technological questions facing the government, congressional and industry sources said.

Given the huge variety of technologies that could be affected -- regular phone service, corporate data transmissions, satellite and microwave communications, and more -- one House staffer said Congress "will have to rent RFK Stadium" to hold hearings.

Marc Rotenberg, a lawyer who has attended meetings with FBI and phone company officials on the proposal, said the FBI, by taking the issue to congressional communications committees, is trying to make an end run around the judiciary committees.

Last year, the Senate Judiciary Committee, responding to civil libertarians' protests, killed an FBI proposal to require that encrypted communications -- such as banks' secret data transmissions -- be made available in decoded form.

Representative Edward J. Markey (D-Mass.), who chairs the House subcommittee handling the latest FBI proposal, said the plan has troubling overtones of "Big Brother" about it.

Let's Blow the Whistle on FBI Phone-Tap Plan March 12, 1992
~~~~~~

Editorial taken from USA Today (Page 6A)

OUR VIEW - Congress should disconnect this unneeded and dangerous eavesdropping scheme as soon as possible
~~~~~~

The FBI -- lambasted in the past for wiretapping and amassing files on thousands of "subversives" such as Martin Luther King -- seems determined to prove that consistency is a virtue.

The Bureau wants phone companies to make costly changes that critics say could let agents eavesdrop on your phone calls without detection -- and boost your phone bill to pay for it.

The FBI says that this new law is needed because it can't wiretap all calls transmitted with the new digital technology. It also wants the public barred when it explains all this to Congress.

Wisely, lawmakers show signs of balking. They're already preparing for high-profile hearings on the proposal.

Congress, though, should go much further. It should pin the FBI's wiretap plan to the wall and use it for target practice. Here are just a few of the spots at which to take aim:

*Rights: The FBI says it is still would get court approval before tapping, but experts say if the agency gets its way, electronic eavesdropping would be far easier and perhaps untraceable. The FBI's plan, they say, could make a mockery of constitutional rights to privacy and against unreasonable searches.

*Need: Some phone companies say they are already meeting FBI wiretap requirements and question whether the agency really needs a new law -- or just would find it convenient. The FBI says it can't tap some digital transmissions -- but it hasn't given any specifics.

*Honesty: The FBI tried to evade congressional review by financing its plan with a charge to phone users.

The bureau must have realized the reception this shady scheme could expect: It tried to slip it though Congress' side door, avoiding the committees that usually oversee FBI operations.

Over the decades, wiretaps have proved invaluable in snaring lawbreakers. Used selectively and restrained by judicial oversight, they're a useful weapon, especially against organized crime.

But if catching gangsters never should take precedence over the rights the Constitution guarantees the citizens who try to follow the law, not break it.

Back to Smoke Signals? March 26, 1992
~~~~~~~~~~~~~~~~~~~~~~

An editorial from The Washington Post

The Justice Department spent years in court breaking up the nation's telecommunications monopoly in order to foster competition and technological advances. Now the same department has gone to Congress asking that improvements in telecommunications technology be halted, and in some cases even reversed, in the name of law enforcement. The problems facing the FBI are real, but the proposed solution is extreme and unacceptable on a number of grounds.

Wiretaps are an important tool in fighting crime, especially the kind of large-scale, complicated crime -- such as drug conspiracies, terrorism and racketeering -- that is the responsibility of the FBI. When they are installed pursuant to court order, taps are perfectly legal and usually most productive. But advances in phone technology have been so rapid that the government can't keep up. Agents can no longer just put a tap on phone company equipment a few blocks from the target and expect to monitor calls. Communications occur now through regular and cellular phones via satellite and microwave, on fax machines and computers. Information is transmitted in the form of computer digits and pulses of light through strands of glass, and none of this is easily intercepted or understood.
~~~~~~~~~~~~~~~~~~~~~~

The Justice Department wants to deal with these complications by forbidding them. The department's proposal is to require the Federal Communications Commission to establish such standards for the industry "as may be necessary to maintain the ability of the government to lawfully intercept communications." Any technology now in use would have to be modified within 180 days, with the costs passed on to the rate payers. Any new technology must meet the suitable-for-wiretap standard, and violators could be punished by fines of $10,000 a day. As a final insult, commission proceedings concerning these regulations could be ordered closed by the attorney general.

The civil liberties problems here are obvious, for the purposeful designing of telecommunications systems that can be intercepted will certainly lead to invasions of privacy by all sorts of individuals and organizations operating without court authorization. Further, it is an assault on progress, on scientific endeavor and on the competitive position of American industry. It's comparable to requiring Detroit to produce only automobiles that can be overtaken by faster police cars. And it smacks of repressive government.

The proposal has been drafted as an amendment rather than a separate bill, and there is some concern that it will be slipped into a bill that has already passed one house and be sent quietly to conference. That would be unconscionable. We believe, as the industry suggests, that the kind of informal cooperation between law enforcement agencies and telecommunications companies that has always characterized efforts in the past, is preferable to this stifling legislation. But certainly no proposal should be considered by Congress without open and extensive hearings and considerable debate.

The FBI's Latest Idea: Make Wiretapping Easier April 19, 1992

By Anthony Ramirez (New York Times)(Section 4, Page 2)

Civil libertarians reacted quickly last month when the Federal Bureau of Investigation proposed new wiretapping legislation to cope with advanced telephone equipment now being installed nationwide.

The FBI, which has drafted a set of guidelines, but has as yet no sponsor in Congress, said the latest digital equipment was so complicated it would hinder the agency's pursuit of mobsters, terrorists and other criminals. But civil liberties groups like the American Civil Liberties Union, joined by several major telephone companies like American Telephone and Telegraph Company, described the proposal as unclear, open to abuse and possibly retarding the pace of technological innovation.

Civil libertarians fear a shift from a world where wiretaps are physically onerous to install, therefore forcing the FBI to think twice about their use, to a world where surveillance is so easy that a few pecks on an FBI key pad would result in a tap of anyone's telephone in the country.

The inventive computer enthusiasts who call themselves hackers are also calling the legislation unnecessary. If teenagers can quickly cope with such equipment, they argue, so can the FBI.

"The easier it is to use, the easier it is to abuse," said Eric Corley, editor of 2600 magazine, a quarterly publication "by and about computer hackers."

According to the FBI, in 1990, the latest year for which data are available, there were 1,083 court-authorized wiretaps -- both new and continuing -- by Federal, state and local law-enforcement authorities. Robert Ellis Smith, publisher of Privacy Journal, said the relatively small number of wiretaps reflects the difficulty of obtaining judicial permission and installing the devices. Moreover, he said, many cases, including the John Gotti case, were solved with eavesdropping devices planted in rooms or on an informant.

Besides, Mr. Smith said, complicated digital equipment shares similarities with obstacles free of technology. "Having a criminal conversation on a digital fiber-optic line," he said, "is no different from taking a walk in the park and having the same conversation." And no one, he added, would think of requiring parks to be more open to electronic surveillance.

At issue are the latest wonders of the telecommunications age -- digital transmission and fiber-optic cables. In the standard analog transmission, changes in electrical voltage imitate the sound of a human voice. To listen in, the FBI and other agencies attach a device to a line from a telephone pole.

A Computer Hiss or Nothing

Today phone systems are being modernized with high-speed, high-capacity digital lines in which the human voice is converted into computer code. Moreover, a fiber-optic line in digital mode, which carries information as pulses of light, carries not only clear conversations but a myriad of them. Using a wiretap on a digital line, FBI agents would hear only a computer hiss on a copper cable, nothing at all on a fiber-optic line.

There are at least 140 million telephone lines in the country, and more than half are served in some way by digital equipment, according to the United States Telephone Association, a trade group. However, less than 1 percent of the network is fiber optic.

The legislation proposed by the FBI would, in effect, require the licensing of new telephone equipment by the Federal Government so the agency could wiretap it. Telephone companies would have to modify computers and software so that agents could decipher the digital bit stream. The cost of the modification would be passed on to rate payers.

"Phone companies are worried about the sweep of this legislation," said Jerry Berman, director of the Electronic Frontier Foundation, who solicited the support of the phone companies for a protest letter to Congress. By requiring the FCC to clear new technology, innovation could be slowed, he said. "We're not just talking about just local and long-distance calls," Mr. Berman said. "We're talking about CompuServe, Prodigy and other computer services, electronic mail, automatic teller machines and any change in them."

Briefcase-Size Decoders

One telecommunications equipment manufacturer said he was puzzled by the FBI proposal. "The FBI already has a lot of technology to wiretap digital lines," he said, on condition of anonymity.

He said four companies, including such major firms as Mitel Corporation, a Canadian maker of telecommunications equipment, can design digital decoders to convert computer code back into voice. A portable system about the size of a large briefcase could track and decode 36 simultaneous conversations. A larger system, the size of a small refrigerator, could follow up to 1,000 conversations. All could be done without the phone company.

James K. Kallstrom, the FBI's chief of technology, acknowledged that the agency was one of Mitel's largest customers, but said the equipment hackers and others describe would be "operationally unfeasible."

The FBI was more worried about emerging technologies like personal communications networks and services like call forwarding. "Even if we used the equipment the hackers say we should use," Mr. Kallstrom said, "all a criminal would have to do is call-forward a call or use a cellular telephone or wireless data transfer to defeat me."

==Phrack Inc.==

Volume Four, Issue Thirty-Eight, File 12 of 15

```
PWN ^*^ PWN ^*^ PWN ^*^ { CFP-2 } ^*^ PWN ^*^ PWN ^*^ PWN
^*^                                                   ^*^
PWN         P h r a c k   W o r l d   N e w s         PWN
^*^         ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~         ^*^
PWN             Special Edition Issue Six             PWN
^*^                                                   ^*^
PWN          Computers, Freedom, & Privacy II         PWN
^*^                                                   ^*^
PWN                 March 18-20, 1992                 PWN
^*^                                                   ^*^
PWN               Written by Max Nomad                PWN
^*^                                                   ^*^
PWN ^*^ PWN ^*^ PWN ^*^ { CFP-2 } ^*^ PWN ^*^ PWN ^*^ PWN
```

Computers, Freedom, & Privacy II
Random Notes and Mission X Telegraphs from the Nation's Capitol

by Max Nomad

Originally, when I read the brochure on the second "Computers, Freedom, and Privacy Conference," I saw opportunity knocking at my door: Three days at the Loew's L'Enfant Plaza Hotel in Washington, D.C. stalking around a series of meetings all geared toward telecommunications, as well as the high potential for mischief; techno-gurus, privacy advocates, computer outlaws, corporate bigwigs, and lastly feds, a few of which who were casually walking around with automatic weapons disguised as black tote-bags. There was no telling what those hackers were capable of, I'm sure, so the beefed up security was necessary.

Upon learning that Basil Rouland, Inc., an information systems security firm, had secured a press pass and transportation, my excitement grew. I wasn't sure what kind of story I would bring back from the trip, or if I would find a unique story at all. Fortunately, the conference topics provided dozens of angles to take on, more than I care list. My previous article and notes alone on the event were upwards of 25k, mostly filled with mundane excerpts and quotes from various panelists. If you're interested in a blow-by-blow account of CFP-2, it's available on VHS; contact bkoball@well.sf.ca.us for more details.

For the readers of PHRACK, a different perspective was in order. The following commentary has been taken strictly from my notes and thoughts on the underground showing.

Overall, this year's CFP was a success. The panel discussions on everything >from the issues of privacy to Internet to cryptography and security were informative, even enlightening. After three days of non-stop conferences on these subjects I realized just how much of a runaway horse technology is to our federal government. Big Brother is definitely out there, but he's got fast competition coming up from the private sector. And special thanks to CRAIG NEIDORF, who graciously donated his name to modern science and the EFF. This individual's case was referred to more times than Roe v. Wade; personally, Craig, if I were you, I'd put a trademark on it and charge by the usage. In any case, this year's CFP conference was a success. Congrats are in order for the organizers and volunteers. Anyone who is seriously interested in computer networks, security, and what the big fish are up to should attend. Also, members of the press are welcome.

Daily, in the aftermath of the conferences, "Birds of a Feather" sessions were held in the meeting rooms. At best, these were well structured discussions for people of similar interests. At worst, they were lame farces, such as the "Why Don't They Understand" discussion, where unofficial representatives of the underground were given a forum to supposedly voice their opinions.

The panel consisted of Glen Tenney (organizer of the annual Hacker's conference), Knight Lightning (founder of Phrack, abused civil rights poster

child for the EFF), Dispater (current publisher of Phrack), Emmanuel Goldstein (editor/publisher of 2600 magazine, host of "Off the Hook" [WBAI radio, New York]), Phiber Optik (hacker/phreak currently receiving a great deal of "fan harassment" by the authorities), Steven Levy (MacWorld, author of _Hackers_), Dorothy Denning (Computer Science Department, Georgetown University), and the panel chair was John McMullen of McMullen & McMullen. Aside from a few hackers and law officials in the audience, the curious and uninformed filled the meeting room to capacity. There was definitely a sense of anticipation prior to the start of the discussion; it didn't take a private eye to know that one way or the other, this was going to be a show.

And it was.

Steven Levy gave a neutral dissertation to the meaning of the word "hacker" as it was when he published his book by the same name back in 1986: programmers and electronics hobbyists supposedly with purer intentions, many of which that went on to make revolutionary waves in the computer industry. Hackers and phone phreaks like Wozniak and Jobs are two of those heroes of yesteryear's underground. But as with the rest of society, nostalgia always casts a darker tint on the present. Those heroes would be considered the maniacal high-tech terrorists of today, thanks to a combination of media sensationalism, a few malicious idiots on both sides of the law, and the general public opinion that hackers are to be feared like hardened outlaws -- all of which stems from varying degrees of ignorance.

Dorothy Denning appended Levy's statement with an objective view, pointing out the fact that neither side seems to fully understand what it's like to walk in the other's shoes, befitting the title of the next session. Another perfect neutrality. Tenney interjected with a somewhat polished speech about what it was to be a hacker (i.e. programmer) back in his day, uttered a few slants directed at certain people, both of which smoothly establishing the slight anti-hack tone that would end up carrying on until this session ended. Upon finding out this man is supposedly running for Congress in some state, I was even less surprised. It was as if he smelled what the crowd wanted to hear, then cooked it up enough to feed everyone. He's pretty good. He'll probably get the seat he's shooting for.

In his best radio voice, Emmanuel Goldstein immediately returned the volley to previous statements, also adding a few interpretations of his own: the feeling of learning and exploring, even in forbidden regions, how it is unhealthy to put restrictions on thought and discovery, and how it is the complacency of the other side that the underground is making use of. He also brought up a very good point concerning the Dutch and how many of the system administrators over there are making use of hackers in the bullet-proofing of their systems. The distrust of most American sysadmins along with the level of arrogance in some cases almost makes such cooperation ludicrous over here in the states. Shame.

Each underground member of the panel eventually made his or her statement, including Phiber Optik's tale of how a certain New York State Police officer and gang rolled up on his home like the DEA and awakened him from his sleep at gun point. Whether by coincidence or not, the officer in charge of the arrest was standing in the back of the room. Of course, the voice of authority had to make a statemental come-back on the topic. In that instant it became obvious that having hacks and law enforcement in the same room wasn't the best vehicle for accurately portraying views. Neither side was prone to be open and honest with the other watching with anticipation. Any hack who was not under investigation wouldn't dare open up and speak, and any hack currently under investigation couldn't speak honestly; no one wants to speak his piece bad enough to get indicted. The feds were in the same boat, since they couldn't openly discuss any pending cases, as well as keeping a lid on any of their trade secrets; a catch-22 that further solidified the misconceptions of those in the middle: the image of hackers as chaotic compu-hoodlums and law enforcement officials as determined yet uninformed trackers.

In all honesty, this session came off like a side show, and the hackers like circus freaks. With two prominent underground publishers, an ex-hack/publisher turned representative of the EFF, and a hack/phreak currently under investigation, there was no alternative but to stutter and give vague answers to delicate questions and even then that only applied to those occasions where they could speak their minds uninterrupted. Self-preservation and the

felonious core of this topic made every answer a forfeited one before it was given. Any well-informed spectator knew this. So did the feds, who were probably chuckling to themselves the entire time. Absolutely no resolutions were made either way. Truthfully, the feds gained brownie points on this one. The hacker perspective wasn't accurately presented and the masses would continue to live ignorance of the underground.

The next night, random reports of strange activity churned through the rumor mill shortly after the hackers hijacked one of the meeting rooms for Knight Lightning's "Frank" Party, the kind of talk most people weren't bold enough to investigate or so "unthinkable" that no one wanted their name attached. The room itself was easy to identify -- "Fire Line Do Not Cross" tape covered the front doors, as well as a chaotic chatter that roared from within. There was no agenda to speak of. Most of the hackers I've met during my travels were leaders and rugged individualists and here was no different. None wanted to take charge -- to do so would have been useless. Each generally did his own thing and, if it looked interesting enough, others would follow. Some of the name-tagged feds would have probably wandered in if they weren't already having a session of their own. Speculatively, they were discussing matters about targeted individuals present at our gathering.

The evening's entertainment was an old cult-classic tape, Frank & The Phunny Phone Call, the hilarious and unexpurgated recordings of an old man driven to aggravated dementia by some anonymous phone phreaks making his phone "go berzerk." Earlier at one of the literature tables, free promotional 2-in-1 screwdrivers were given away (a gift from Hayes Modem Corporation) and it seemed that every hack in here had at least one or two. Granted, these tools are handy for any computer buff, but a room full of hacks and phreaks with them was almost as unpredictable as handing out matches at a Pyromaniacs Anonymous meeting. Soon, RJ-11 phone jacks were being unscrewed from the wall and studied. Lineman's Test Phones appeared, soon followed by a small expedition stalking around the service hallways and finding the unlocked telephone closet for the hotel. The rest is, shall we say, up to reader interpretation as to what happened after that, ironically ten yards and a set of double doors away >from a room full of state cops and feds.

The Last Day

Instead of rushing the microphone during the final statements in the main conference room, our rogue gang had coagulated in the hall (next to the payphones no less) around an Air Force special investigator and Phiber Optik. At first the mood resembled that of a James Bond movie, where Bond and an arch nemesis would meet and chat, each anticipating the downfall of the other beneath polite exteriors. This seemed to be the sublime tension between all the feds and hacks who talked at the conference, but it was especially delicate in this case -- Phiber was high on the priority list this agent's department was currently investigating. Eventually the mood lightened, and an impromptu Q&A pow-wow session between the hacks and the agent broke out, spawning all sorts of conversations that seemed much more interesting than the finale taking place inside. And, like clockwork, a little mischief came into play. As a show of good faith and a sign that the hackers would be returning for next year's conference, several prominent organizers found that the answer messages on their hotel voice mailboxes had been mysteriously "changed." Sources say the culprit was described as an old Yiddish, but all reports on this matter were unconfirmed. Shortly after this impromptu gathering, it was apparent that the conference had finally adjourned. Except for the underground types and a few observers, the halls were thinning out, and eventually we all wandered our separate ways. And once again, this environment began to take the look of a hotel.

To The Underground At Large:

This was just one conference; the feds will continue to do what they do and so will we. After the hacker panel fiasco, I overheard John Markoff (New York Times reporter and co-author of the book _Cyberpunk_) and Steve Levy talking about how topics like this were being discussed in conferences like this ten years ago. Only the names and circumstances had changed -- the song and dance steps remained the same. Chances are, ten years from now these same subjects

will share some portion of the limelight in regard to growth and development of cyberspace. As society becomes more technologically complex, the bugs, loopholes, and defaults will exist and the underground will thrive. Whether the masses choose to acknowledge this or not, we are a subculture of and to ourselves, much like the Grateful Dead followers. Some will move on, die off, or fade away, and others will stream in to fill the empty spaces. A few words of interpretive advice to the newbees: study everything you touch carefully, covet and respect the knowledge you gain like a gun, and never drive faster than you can think. The feds are out there and, trust me, these motherfuckers didn't come to play.

To The Feds And Hacker Trackers Present At The Conference:

There isn't much that can be said. You have a much better understanding of the computer underworld than most, even than by some of those in it. By virtue of the job you do, this is a given. Respect is due to you for your showing at CFP-2, how you presented yourselves, and the subtle way you furthered the brainwashed concepts of "the hacker" in the public eye. You knew the presentations would be slanted in your favor, and probably took great pride in this. Smooth. Very smooth.

To The Uninformed:

Don't blindly believe the hype. Whether you wish to face it or not, hackers and phone phreaks are an integral part of this technological revolution. Advancement cannot come without the need for change and to improve, both micro- and macroscopically. Positive direction is the result of an equal but opposite force that presses it forward. Because of the hackers (old, new, and even the malicious), software and hardware developers have made radical improvements on the networks and supermachines that are undeniably molding the foundation of tomorrow's world. Our society is based on complacency. And any social institution or machinery that seems to work without weight to tip the scales of change simply goes unchecked, eventually to become a standard. The hijinx that Congress gets away with and how little the public truly reacts is a perfect example. If hackers didn't truly love computers and telecommunications or have an unnatural need to explore and learn, the technological growth curve would be stunted. Long after these embryotic times have faded into our grandchildren's history books, hackers will exist, and the bulk of high-tech crimes will continue to be perpetrated by minions of the people in power, the elite white-collar.

Regardless of the long-term insight, computer intrusion is still an illegal art and science.

There is no rationale for why hackers hack, at least nothing that will withstand the scrutiny of the unenlightened masses or one's inner beliefs. "Hackers," like any other subculture, yield a range of personalities and perspectives from the careful explorer to the callous marauder. Inexperienced sociologists would probably try to classify this underground sect as a movement, possibly even subversive in its intentions. The problem with this lies in the fact that a movement needs a leader or spokesman. Aside from the individual nature of these people, anyone who becomes a mouthpiece for this culture cannot rightly be a hacker, or at least hacking around with anything unlawful. Chances are, others would shy away from such a person, seeing him as either an informant or too dangerous to be around; the feds would pursue him passionately, like tracking a trophy-sized bull in a deer hunt. Hackers cannot be categorized as a movement, fad, or pre-packaged subculture like bubble-gum rock music or the pseudo-hippies of the 90's. Most hackers have their own directions and forward momentum. It is a shared mindset, ironically paralleling that of the feds that chase them. One group has no rules or set channels to adhere to. The other is backed by the establishment and a badge.

This statement was not intended to rationalize their actions, only give insight to the uninitiated. To summarize the spectrum of motives with the hacker intellect, I give this analogy: the need to come onto someone else's property, some for peaceful exploration, others to inhabit, and in some instances to misuse or destroy is not a new phenomena. The early settlers of this country did the same thing to the Native Americans.

I\/Iax I\Iomad

[Mission X Tribe Out]

[---------]

Thanks and respect are due to:

Basil Rouland Inc. (for getting me there) and URban Lividity, Jet Heller, Silkworm, and the rest of the "In The Flesh" (804-489-7031) posse that couldn't make the trip. mXt.

==Phrack Inc.==

Volume Four, Issue Thirty-Eight, File 13 of 15

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN      Issue XXXVIII / Part One of Three      PWN
PWN                                             PWN
PWN        Compiled by Dispater & Friends       PWN
PWN                                             PWN
PWN     Special Thanks to Datastream Cowboy     PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Warning: Multiplexor/The Prisoner Tells All — April 10, 1992

On approximately April 3, 1992, Multiplexor (a/k/a The Prisoner) illegally used credit card information obtained from CBI/Equifax to purchase an airline ticket to San Diego, California from his home in Long Island, New York. Upon his arrival, MP was met by several agents of the Federal Bureau of Investigation.

After his apprehension, MP was taken first to a computer store where agents allegedly picked up a computer from the store manager who is a friend of either one of the agents or a federal prosecutor involved in the case.

At the taxpayer's expense, Multiplexor was put up for at least a week at a Mariott Hotel in San Diego while he told all that he ever knew about anyone to the FBI. It is believed that "Kludge," sysop of the San Diego based BBS Scantronics has been implicated, although reportedly his board does not contain ANY illegal information or other contraband.

It is widely known that card credit abusing scum like Multiplexor are inherently criminal and will probably exaggerate, embellish and otherwise lie about other people in order to escape prosecution themselves. If you have ever come into contact with Multiplexor -- beware. He may be speaking about you.

Incidentally, Multiplexor had this year submitted a poorly written and ill-conceived article to Phrack about voice mail hacking. His article was denied publication.

And now this is the final result...

Nationwide Web of Criminal Hackers Charged — April 20, 1992

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

San Diego -- According to a San Diego Union-Tribune report, San Diego police have uncovered "an electronic web of young computer hackers who use high-tech methods to make fraudulent credit card charges and carry out other activities."

The Friday, April 17th story by Bruce V. Bigelow and Dwight C. Daniels quotes San Diego police detective Dennis Sadler as saying that this informal underground network has been trading information "to further their political careers." He said that the hackers know how to break computer security codes, create credit card accounts, and make fraudulent credit card purchases. Sadler estimated that as many as 1,000 hard-core hackers across the United States have shared this data although he said that it's unclear how many have actually used the information to commit crimes.

Sadler added that he estimated that illegal charges to credit cards could total millions of dollars.

While the police department did not release details to support the allegations, saying that the investigation is continuing, Sadler did say that cooperation >from an "out-of-state hacker," picked up in San Diego, provided important information to the police and the FBI. Although police would not release the identity of this individual or his present whereabouts, information gathered

by Newsbytes from sources within the hacker community identifies the so-called hacker as "Multiplexer", a resident of Long Island, NY, who, according to sources, arrived in San Diego on a airline flight with passage obtained by means of a fraudulent credit card purchase. The San Diego police, apparently aware of his arrival, allegedly met him at the airport and took him into custody. The same sources say that, following his cooperation, Multiplexer was allowed to return to his Long Island home.

The Union-Tribune article linked the San Diego investigation to recent federal search and seizures in the New York, Philadelphia and Seattle areas. Subjects of those searches have denied to Newsbytes any knowledge of Multiplexer, illegal credit card usage or other illegal activities alleged in the Union-Tribune story. Additionally, law enforcement officials familiar with on-going investigations have been unwilling to comment, citing possible future involvement with the San Diego case.

The article also compared the present investigation to Operation Sun-Devil, a federal investigation into similar activities that resulted in a massive search and seizure operation in May 1990. Although individuals have been sentenced in Arizona and California on Sun Devil related charges, civil liberties groups, such as the Computer Professionals for Social Responsibility, have been critical about the low number of criminal convictions resulting from such a large operation.

Sun-Devil Becomes New Steve Jackson Game March 25, 1992
~~~~~~

By Steve Jackson

It couldn't have been more than a week after the initial raid when people started saying, "Hey, why don't you make a game out of it?" The joke wore thin quickly, as I heard it over and over and over during the next year. Then I realized that I was in serious danger of losing my sense of humor over this... and that actually, it would be possible to do a pretty good game about hacking. So I did.

In 1990, the Secret Service raided Steve Jackson Games when a "hacker hunt" went out of control. Loss of our computers and unfinished game manuscripts almost put this company out of business.

It's been two years. We're back on our feet. And ever since the raid, fans have been asking, "When are you going to make a game out of it?"

Okay. We give up. Here it is.

The game has enough fanciful and pure science-fiction elements that it's not going to tutor anyone in the arcane skills. Neither is it going to teach the sysadmin any protective tricks more sophisticated than "don't leave the root set to default." But it is, I think, a good simulation of the *social* environment of High Hackerdom. You want to outdo your rivals -- but at the same time, if you don't share knowledge with them, you'll never get anywhere. And too many wannabes on the same system can mess it up for everybody, so when you help somebody, you ask them to try it out *somewhere else* . . . and occasionally a hacker finds himself doing the sysadmin's housecleaning, just to preserve his own playground against later intruders. I like the way it plays.

In HACKER, players compete to invade the most computer systems. The more systems you crack, the more you learn, and the easier the next target is. You can find back doors and secret phone lines, and even crash the systems your rivals are using. But be careful. There's a Secret Service Raid with your name on it if you make too many enemies.

Designed by Steve Jackson, the game is based on the award-winning ILLUMINATI. To win at HACKER requires guile and diplomacy. You must trade favors with your fellow hackers -- and get more than you give away. But jealous rivals will try to bust you. Three busts and you're out of the game. More than one player can win, but shared victories are not easy!

HACKER is for 3-6 players. Playing time is under an hour for the short game and about 2 hours for the regular game. Components include a rule book, 110
~~~~~~

cards, marker chips, 6 console units, system upgrades, Bust markers, and Net Ninja marker, two dice and a Ziplock bag.

Hacker began shipping March 30, and has a suggested retail price of $19.95.

"Peter The Great " Had An Overbyte January 10, 1992

By Kay Kusumoto (The Seattle Times)(Page B1)

"Teenage Hacker Ring Bigger Than Thought"

Bellevue, Washington -- Imagine you're a 17-year-old computer whiz who has figured out how to get into the phone-company computer to make long-distance calls for free.

Imagine finding at the tip of your fingers step-by-step instructions on how to obtain credit-card numbers.

And imagine once more the name you use to log on to a computer system isn't really your own, but actually a tag, or moniker -- like, say, that of a Russian czar.

Bellevue police say that's the name an Issaquah teenager used when sending messages to fellow hackers all over the country.

They first arrested "Peter the Great" a month ago for investigation of attempted theft in using an unauthorized credit-card number to try to purchase a $4,000 computer from a store in Bellevue.

But now police, who are still investigating and have not yet filed charges, believe they're on to something much larger than first suspected. They say they are looking for one or two additional youths involved with the 17-year-old in a large computer-hacking ring that uses other people's credit-card numbers to purchase computers and software.

In the youth's car, police say, they found another $4,000 computer obtained earlier that day from a Seattle computer store. They also claim to have found documents suggesting the youth had used credit information illegally.

Police Lt. Bill Ferguson of Bellevue's white-collar crime unit said detectives don't know how many people are involved in the scam or how long it has been going on. And police may never know the dollar loss from businesses and individuals, he said.

"You can guess as high as you want," Ferguson said. "He had connections clear across the country."

After the youth was arrested, police say, he admitted to being a hacker and using his parents' home computer and telephone to call boards.

An elaborate type of e-mail -- the bulletin boards offer the user a electronic messaging -- system, one may gain access to a "pirate" bulletin directory of "how to" articles on ways of cracking computer systems containing everything >from credit records and phone accounts to files in the University of Washington's chemistry department.

Once the youth decided which articles he wanted most, he would copy them onto his own disk, said Ferguson. Now police are poring over hundreds of disks, confiscated from his parents' house, to see just how much information he had. The parents knew nothing of what was going on, police say. Ferguson said police also seized a copy of a New York-based magazine called 2600, aimed at hackers. Like the bulletin boards, the magazine provides readers with a variety of "how to" articles.

The teenager, who was released to his parents' custody the day of his December 3 arrest, told police the magazine taught him how to use a device that can imitate the sound of coins dropping into a pay phone. With that, he could dial outside computers for free.

Police confiscated the device.

"Hackers are difficult to trace because they don't leave their name on anything," Ferguson said, adding that a federal investigation may follow because detectives found copies of government documents on the youth's disks.

"This kid (copied) hundreds of pages of articles, left messages and shared (computer) information with other hackers," said Ferguson.

"What's common about the hacker community is that they like to brag about their accomplishments -- cracking computer systems. They'll tell each other so others can do it."

- -

Hotel Credit Doesn't Compute January 22, 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~

By Stephen Clutter and Kay Kusumoto (The Seattle Times)(Page D1)

"Kirkland Police Suspect Hacker"

Kirkland, Washington -- Police are investigating yet another potential computer hacking case, this one at the Woodmark Hotel in Kirkland.

Someone, according to hotel officials, got into the Woodmark's computer system and gave themselves a $500 credit for a hotel room earlier this month.

Police say a 19-year-old Bellevue man is the main suspect in the case, although no arrests have been made.

The incident surfaces at the same time as Bellevue police press their investigation into their suspicions that a 17-year-old Issaquah youth, using the computer name "Peter the Great," got access to credit-card numbers to purchase computers and software. That suspect was arrested but is free pending charges.

"The deeper we get into Peter's files, the more we're finding," Bellevue police Lt. Bill Ferguson said.

After arresting the youth last month on suspicion of trying to use an unauthorized credit-card number to purchase a $4,000 computer from a Bellevue store, police confiscated hundreds of computer disks and have been searching the electronic files for evidence.

"We've been printing one file out for three hours now -- and it's still printing," Ferguson said yesterday.

The file, Ferguson estimated, contains at least 10,000 names of individuals, with credit-card numbers and expiration dates, addresses, phone numbers and Social-Security numbers.

Detectives will meet with the Bellevue city prosecutor later this week to discuss charges.

In the Kirkland incident, the 19-year-old Bellevue man stayed in the hotel the night of January 11, according to Kirkland Detective Sgt. Bill O'Brien.

The man apparently made the reservation by phone a few days earlier and was given a confirmation number. When he went to check into the hotel on January 11, the receptionist found that a $500 credit had been made to his room account, O'Brien said.

Woodmark officials, fearing they had a hacker problem, contacted Bellevue police last week after reading news accounts of the arrest of "Peter the Great."

"The hotel said they had read the story, and discovered what appeared to be a break-in to their computer system," said Ferguson. "They wanted to know if maybe it was related to our "Peter the Great" case."
~~~~~~~~~~~~~~~~~~~~~~~~~~~

Police don't know, Ferguson said -- and that's one of the things under investigation.

The main suspect in the Woodmark case had worked at the hotel for five days in 1990, police say, and may have had access to the hotel's computer access code. Hotel officials suspected they had a hacker on their hands because phone records indicate that the $500 credit was made via a telephone modem and not by a keyboard at the hotel, Ferguson said. The problem was discovered after an audit showed the $500 was never paid to the hotel.

So what happened during the free night at the Woodmark?

"They partied and made various phone calls, including nine to the University of Washington," O'Brien said.

The calls to the university went to an answering machine at the Medical Center, police say, and there is no indication the men were able to hack their way into the university's computer system.

They were up to something, though, and police want to know what. "We're going to start with the (19-year-old Bellevue) kid, and start from there," O'Brien said.

- -

Hacker Charged With Fraud February 14, 1992
~~~~~~~~~~~~~~~~~~~~~~~~~

By Kay Kusumoto (The Seattle Times)(Page F3)

"Teen Computer Whiz May Be Part Of A Ring"

"Peter the Great" played courier for "Nighthawk."

He was supposed to pick up a couple computers purchased with an unauthorized credit-card number from a computer store in Bellevue, Washington last December.

He never finished the transaction. A suspicious clerk called police and "Peter" was arrested for attempted theft.

But that was only the beginning.

The Issaquah teenager who went by the computer name "Peter the Great" was charged yesterday in King County Juvenile Court with attempted theft, possession of stolen property, telephone fraud and computer trespass..

The arrest of the 17-year-old computer whiz led Bellevue police on an investigation into the underground world of computer hacking.

Police are still investigating the case and say they believe it involves members of a large computer-hacking ring who use other people's credit-card numbers to purchase computers and software.

Court documents allege the youth was after two $1,800 computers on December 3, 1991, the day he walked into a Bellevue computer store to pick up an order for an unknown associate who went by the hacker moniker "Nighthawk."

The computers had been ordered with a credit-card number given over the phone by a man identifying himself as Manuel Villareal. The caller told the clerk that another man named Bill Mayer would pick up the order later in the day.

But a store clerk became suspicious when the youth, who said he was Bill Mayer, "appeared very nervous" while he was inside the store, court papers state.

When the youth couldn't provide enough identification to complete the transaction, the clerk told him to have Villareal come into the store and sign for the computers himself.

After the youth left, the clerk called police, and "Peter" was arrested later that day.
~~~~~~~~~~~~~~~~~~~~~~~~~

A search of his car revealed a torn up VISA card, several computer disks, two more computers, a receipt from a computer store in Seattle and several pieces of paper with credit-card numbers on them, court papers state.

The youth also had in his possession a red box, a device that simulates the sound of coins dropping into a pay phone.

After his arrest, the youth told police that "Nighthawk" had telephoned the computer store and used Villareal's name and credit-card number to make the purchase in Bellevue.

The teen admitted to illegally using another credit-card number to order a computer from a store in Seattle. The computer was picked up later by another unknown associate.

The youth also told police that another associate had hacked his way into the computer system of a mail-order house and circulated a list of 14,000 credit card numbers through a computer bulletin board.

Computer Hackers Nabbed January 29, 1992
~~~~~~~~~~~~~~~~~~~~~~~

By Michael Rotem (The Jerusalem Post)

Four computer hackers were arrested and their equipment seized in raids by police and Bezek security officers on four homes in the center and north of the country. They were released on bail yesterday after questioning.

The four, two minors and two adults, are suspected of purloining passwords and then breaking the entry codes of international computer services and toll-free international telephone switchboards, stealing thousands of dollars worth of services.

The arrests were made possible after National Fraud Squad officers joined Bezek's efforts to discover the source of tampering with foreign computer services.

A Bezek source told The Jerusalem Post that all four suspects had used personal computers and inexpensive modems. After fraudulently obtaining several confidential passwords necessary to enter Isranet -- Israel's national computer network -- the four reportedly linked up to foreign public data banks by breaking their entrance codes.

This resulted in enormous bills being sent to the password owners, who had no idea their personal secret access codes had been stolen.

The four are also suspected of illegally obtaining secret personal credit numbers used by phone customers to call abroad. The suspects reportedly made numerous telephone conversations abroad worth thousands of shekels.

A police spokesman said cooperation between Bezek's security department and the police National Fraud Squad will continue, in order to "fight these felonies that cause great financial damage." Bezek spokesman Zacharia Mizrotzki said the company is considering changing the secret personal passwords of network users on a frequent basis.

Hackers Get Free Credit February 24, 1992
~~~~~~~~~~~~~~~~~~~~~~~

By Doug Bartholomew (Information Week)(Page 15)

Banks and retail firms aren't the only ones peeking at consumers' credit reports. Equifax Inc., one of the nation's three major credit bureaus admitted that some youthful computer hackers in Ohio had penetrated its system, accessing consumers' credit files. And if it wasn't for a teenager's tip, they would still be at it.

"We do not know how the hackers obtained the access codes, but we do know the confidentiality requirements for membership numbers and security pass-codes were breached," says a spokesman at Equifax. The company, which had revenue of

$1.1 billion in 1991, possesses a database of some 170 million credit files.

A customer number and access code must have been given to the teenagers, or stolen by them, adds the spokesman, who says Equifax "plans to increase the difficulty of accessing the system." Theft of computer access codes is a federal crime.

Virtually No Protection

Critics of the credit agencies say such breaches are common. "There is virtually no protection for those systems," says a spokesman for the Computer Professionals for Social Responsibility, a Washington association. "If some car salesman leaves the information sitting on his desk, someone could just pick up the codes."

As of last week, Dayton police had made no arrests. But they searched the homes of two young men, age 18 and 15, confiscating half a dozen PCs and numerous floppy disks.

The two are thought by police to be part of a group of up to 50 hackers believed to be behind the systems break-in. The group is also under investigation for allegedly making $82,000 worth of illegal phone calls using an 800 number provided to business customers of LDDS Communications Inc., a long-distance service in Jackson, Mississippi. LDDS was forced to disconnect the 800 number on November 15, 1991.

Two Cornell Students Charged In Virus Attacks February 26, 1992
~~~~~~

By Grant Buckler (Newsbytes)
Also see Phrack 37, File 11 -- Phrack World News

Ithaca, New York -- Charges have been laid against two Cornell University students accused of planting a virus that locked up Apple Macintosh computers at Cornell, at Stanford University in California, and in Japan.

David S. Blumenthal and Mark Andrew Pilgrim, both aged 19, were charged in Ithaca City Court with one count each of second-degree computer tampering, a Class A misdemeanor. The investigation is continuing and additional charges are likely to be laid, said Cornell University spokeswoman Linda Grace-Kobas. Both students spent the night in jail before being released on bail February 25, Grace-Kobas added.

The MBDFA virus apparently was launched February 14 in three Macintosh computer games: Obnoxious Tetris, Tetriscycle, and Ten Tile Puzzle. Apparently, a computer at Cornell was used to upload the virus to the SUMEX-AIM computer archive at Stanford University and an archive in Osaka, Japan.

MBDFA is a worm, a type of computer virus that distributes itself in multiple copies within a system or into connected systems. MBDFA modifies systems software and applications programs and sometimes results in computer crashes, university officials reported.

Reports of the MBDFA virus have been received from across the United States and >from around the world, including the United Kingdom, a statement from the university said.

Judge Orders Hacker To Stay Away From Computers March 17, 1992
~~~~~~

By Jim Mallory (Newsbytes)

DENVER, COLORADO -- A computer hacker who pleaded guilty to breaking into space agency computer systems was ordered to undergo mental health treatment and not use computers without permission from his probation officer.

The 24 year-old man, a resident of suburban Lakewood, was sentenced to three years probation in what is said to be one of only five prosecutions under the federal computer hacker law.

The man pleaded guilty last year to one count of breaking into a National Aeronautics and Space Administration (NASA) computer, after NASA and the Federal Bureau of Investigation agents tracked him down in 1990. Prosecutors said the man had spent four years trying to get into computer systems, including those of some banks.

Prosecutors said the man had gained access to a Defense Department computer through the NASA system, but declined to give any details of that case. The indictment did not explain what had occurred.

In the plea bargain agreement, the man admitted he gained access to NASA's computers "by exploiting a malfunction in a public access NASA computer bulletin board service."

The man was described as an unemployed loner who had spent most of his time using a computer at home. The prosecutor was quoted as saying the man needed counselling "on a social level and for personal hygiene."

- -

Hacker Journeys Through NASA's Secret World March 24, 1992
~~~~~~

By Scripps Howard (Montreal Gazette)(Page A5)

"It became more like a game. How many systems can you break into?"

While tripping through NASA's most sensitive computer files, Ricky Wittman suddenly realized he was in trouble. Big trouble.

He had been scanning the e-mail, electronic messages sent between two scientists at one of NASA's space centers. They were talking about the computer hacker who had broken into the system. They were talking about Wittman.

Curiosity collapsed into panic.

"Logoff now!" 24-year-old Wittman remembers thinking as he sat alone in his apartment, staring at his computer screen, in May 1990. "Hang up the phone. Leave the house."

By then it was too late. The National Aeronautics and Space Administration's computer detectives were on the trail. After 400 hours of backtracking phone records, they found the Sandpiper Apartments in Westminster, Colorado.

And they found the inconspicuous third-floor apartment where Wittman -- using an outdated IBM XT computer -- perpetrated the most massive hacking incident in the history of NASA.

Last week a federal judge sentenced Wittman to three years' probation and ordered him to undergo psychiatric counselling.

But perhaps the most punishing aspect to Wittman was the judge's order that he not use computers without permission from a probation officer.

"That's going to be the toughest part," Wittman said. "I've become so dependent on computers. I get the news and weather from a computer."

In his first interview since a federal grand jury indicted him in September, Wittman expressed regret for what he had done.

But he remained oddly nonchalant about having overcome the security safeguards designed by NASA's best computer minds.

"I'll level with you. I still think they're bozos," Wittman said. "If they had done a halfway competent job, this wouldn't have happened."

Prosecutors didn't buy Wittman's argument.

"No software security system is foolproof," wrote assistant U.S. attorney Gregory Graf. "If a thief picks the lock on the door of your home, is the
~~~~~~

homeowner responsible because he didn't have a pick-proof lock on the front door?"

Breaking into the system was just that easy, Wittman said, so much so that it took him a while to realize what he had done.

He had been fooling around inside a public-access NASA computer bulletin-board service in 1986, looking for information on the space-shuttle program. He started toying with a malfunction.

"The software went blooey and dumped me inside," Wittman said. "At first, I didn't know what happened. I pressed the help key. I realized after a while that I was inside."

Somehow, Wittman -- then 18 -- had found a way to break out of the bulletin board's menu-driven system and into a restricted-access area full of personal files.

Once past the initial gate, it didn't take Wittman long to find the file of a security manager. Wittman picked up a password for another system, and the romp began.

"Then I started looking around, and it became more like a game," he recalled. "How many systems can you break into?"

By the federal government's count, Wittman eventually hacked his way into 115 user files on 68 computer systems linked by the Space Physics Analysis Network. His access extended as far as the European Southern Observatory in Munich, Germany.

Given the chance, Wittman could have gone even farther, prosecutors contend. In an interview with the FBI, Wittman told agents he accidently had come across the "log on" screen for the U.S. controller of the currency. Wittman said he didn't try to crack that password.

"The controller of the currency is a little out of my league," he said.

Georgia Teenage Hacker Arrested March 19, 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

By Jim Mallory (Newsbytes)

LAWRENCEVILLE, GEORGIA -- A Georgia teenager has been arrested on charging of illegally accessing data files of several companies in a attempt to inject a computer virus into the systems.

The alleged computer hacker, who was originally charged with the illegal access charges two weeks ago, was re-arrested on felony charges at his high school this week on the additional charges of attempting to infect the computer systems.

The 18-year old boy allegedly broke into computers of BellSouth, General Electric Company, IBM, WXIA-TV in Atlanta, and two Gwinnett County agencies, who were not identified.

The boy's 53-year-old mother was also arrested, charged with attempting to hinder her son's arrest by trying to have evidence against him destroyed.

Computer users' awareness of computer viruses was heightened recently over the so-called Michelangelo virus, which some computer security experts thought might strike tens of thousands of computers, destroying data stored on the system's hard disk. Perhaps due to the massive publicity Michelangelo received, only a few hundred PCs in the US were struck.

Hackers access computers through telephone lines. Passwords are sometimes obtained from underground bulletin boards, are guessed, or can be obtained through special software programs that try thousands of combinations, hoping to hit the right one.

A recent Newsbytes story reported the conviction of a Denver area resident, who
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

was sentenced to three years probation and ordered not to use computers without permission after attempting to break into a NASA (National Aeronautics and Space Administration) computer.

Officials and victims are usually reluctant to give details of computer break-ins for fear of giving other would-be hackers ideas.

Hacker Surveillance Software March 21, 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~

By Susan Watts, Technology Correspondent for The Independent (Page 6)

"Hacker 'Profiles' May Curb Computer Frauds"

The Federal Bureau of Investigation is dealing with computer hackers as it would rapists and murderers -- by building "profiles" of their actions.

Its computer researchers have discovered that, in the same way that other offenders often favour the same weapons, materials or times of day to perpetrate their crimes, hackers prefer to use trusted routines to enter computer systems, and follow familiar paths once inside. These patterns can prove a rich source of information for detectives.

The FBI is developing a modified version of detection software from SRI International -- an American technology research organization. Teresa Lunt, a senior computer scientist at SRI, said hackers would think twice about breaking into systems if they knew computer security specialists were building a profile of them. At the very least, they would have to constantly change their hacking methods. Ms. Lunt, who is seeking partners in Britain to help develop a commercial version of the software, believes hackers share with psychotic criminals a desire to leave their hallmark.

"Every hacker goes through a process peculiar to themselves that is almost a signature to their work," she said. "The FBI has printed out long lists of the commands hackers use when they break in. Hackers are surprisingly consistent in the commands and options they use. They will often go through the same routines. Once they are in they will have a quick look around the network to see who else is logged on, then they might try to find a list of passwords."

SRI's software, the development of which is sponsored by the US Defense Department, is "intelligent" -- it sits on a network of computers and watches how it is used. The software employs statistical analysis to determine what constitutes normal usage of the network, and sets off a warning if an individual or the network behaves abnormally.

A more sophisticated version of the program can adapt itself daily to accommodate deviations in the "normal" behavior of people on the network. It might, for example, keep track of the number of temporary files created, or how often people collect data from an outside source or send out information.

The program could even spot quirks in behavior that companies were not expecting to find.

The idea is that organizations that rely on sensitive information, such as banks or government departments, will be able to spot anomalies via their computers. They might pick up money being laundered through accounts, if a small company or individual carries out an unusually large transaction.

~~~~~~~~~~~~~~~~~~~~~~~~~~~

==Phrack Inc.==

Volume Four, Issue Thirty-Eight, File 14 of 15

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN      Issue XXXVIII / Part Two of Three      PWN
PWN                                             PWN
PWN        Compiled by Dispater & Friends       PWN
PWN                                             PWN
PWN     Special Thanks to Datastream Cowboy     PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

What's Wrong With The Computer Crime Statute? February 17, 1992

By Thomas A. Guidoboni (ComputerWorld)(Page 33)

"Defense and prosecution agree the 1986 Computer Fraud and Abuse Act is flawed but differ on how to fix it."

It has become an annual ritual, since the birth of the Internet worm, for Congress to consider amendments to the 1986 Computer Fraud and Abuse Act. At this point, the U.S. Department of Justice can be expected to advocate three things: an expansion of the federal role in the investigation and prosecution of computer crimes, the creation of new categories of offenses, and harsher penalties, including perhaps the current darling of the department, forfeiture of property.

Since the law is of recent origin, was substantially revised in 1986 and proved more than adequate to prosecute and convict Robert T. Morris, there seems little justification for expansion of its coverage.

Nevertheless, if Congress is determined to review and revise the provisions of the act, there are several narrow, but significant, amendments that are clearly warranted. Of primary importance is the definition of terms. The core of the law suffers from a lack of clarity. Offenses are described by reference to "authorized" or "unauthorized access," yet these terms are not defined anywhere.

Perilously Vague

In a universe that consists of broad computer networks, bulletin boards, E-mail and anonymous file-transfer protocols, and one in which permissions and rights are established by custom, usage and private understandings, a person is left to speculate at his peril as to what conduct is permitted and what is prohibited by this vague language.

The Computer Fraud and Abuse Act should be amended to give precise content to the concepts of "access" and "authorization," thereby providing fair warning of illegal conduct.

A second change for the better regarding the act would be to create a distinction between those computer intruders who unintentionally cause a monetary loss and those who maliciously cause such harm.

The present law, as interpreted in the Morris case, recognizes no such distinction. This is contrary to long-standing notions of fairness in our system of criminal law, which acknowledges that between two persons who cause the same harm, the one who intended that result is more culpable than the one who did not.

A third part of the statute that needs revision relates to computerized medical records. It is too broad because it includes as felonious conduct the unauthorized access to such records that "potentially modifies or impairs" medical treatment or care. Virtually every unauthorized access to computers containing medical records carries this potential. A better solution would be

simply to make any "unauthorized access" of computerized medical records data a misdemeanor, with the intentional modification or destruction of such data designated as a felony.

Amend, But Don't Expand

These slight but important amendments would serve to clarify and improve a basically sound law without stifling the creativity of persons akin to those who have been responsible for many of the advances in computer technology in this country. More expansive revisions are ill-advised, as they may unnecessarily encroach on evolving privacy and free-expression interests.

A broadening of federal involvement is also inappropriate. Nearly every state has enacted laws against computer fraud and abuse and, as Congress recognized in 1986, federal jurisdiction should be limited to cases where there is a compelling federal interest. This might include instances where computers belonging to the federal government or to financial institutions are involved, or cases where the crime itself is interstate in nature. Furthermore, other computer crimes should be left to prosecution by the individual states, as is presently the case.

In sum, the 1986 Computer Fraud and Abuse Act would benefit from some clarification, but expansion of its coverage and wholesale revisions are both ill-advised and unnecessary.

Note: Thomas A Guidoboni is an attorney with Bonner & O'Connell in Washington, D.C. He represented Robert T. Morris in the Internet virus case.

Private Social Security Data Sold to Information Brokers February 29, 1992

By R.A. Zaldivar (San Jose Mercury News)

Washington, D.C. -- The privacy of 200 million Americans with records at the Social Security Administration is threatened by an illegal trade in pilfered computer files. Computerization has dramatically improved our ability to serve the public," Social Security Deputy Commissioner Louis Enoff told a Senate panel. "However, it has also made confidentiality more difficult."

Two executives of Nationwide Electronic Tracking, a Tampa, Florida, company, pleaded guilty to conspiracy charges in January for their part in a national network selling Social Security records. Twenty-three people, including agency employees and police officials, have been indicted in the case -- the largest known theft of government computer data. "Information brokers" will pay Social Security employees $25 for a person's earnings history and then sell the data for as much as $300. Their growing list of customers includes lawyers, private investigators, employers, and insurance companies.

Social Security records contain a mother lode of information that includes not only a person's past earnings but names of employers, family history and even bank account numbers of people who receive benefits by direct deposit. The information can be used to find people or to make decisions on hiring, firing, suing or lending, said Larry Morey, deputy inspector general of the Health and Human Services Department.

"Here we have a large-scale invasion of the Social Security system's confidentiality," said Senator Daniel P. Moynihan, D-N.Y., chairman of the Social Security subcommittee.

Information from other government data bases with records on individuals -- such as the FBI's National Criminal Information Center -- is also available on the underground market. All a broker needs is the cooperation of a clerk at a computer terminal.

Congress may revise privacy laws to increase penalties for illegally disclosing information in the private files of individuals.

Enoff said Social Security is studying ways to improve computer security, as well as keeping closer tabs on employees with access to files, and stressing to its workers that unauthorized disclosure of information is a federal crime.

- -

Related articles can be found in Phrack World News, Issue 37, Part One:

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

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

Back to Act I March 3, 1992
~~~~~~~~~~~~~
Taken from Communications Daily (Page 2)

"Supreme Court Lets Stand Ruling That FCC Ban On Indecency Is Unconstitutional"

FCC's 24-hour ban on indecent programming is unconstitutional, U.S. Supreme Court ruled in refusing to consider unanimous U.S. Appeals Court, D.C., decision. Supreme Court action also effectively overruled December 1988 rider to Senate appropriations bill directing FCC to ban all indecent programming. Last summer, en banc Appeals Court had refused to reconsider May decision by unanimous 3-judge panel that FCC ban is unconstitutional.

FCC, with support of Justice Department, had asked Supreme Court to reconsider case. Coalition of 14 intervenors, including Action for Children's TV (ACT), had opposed FCC in Appeals Court and Supreme Court. En banc Appeals Court said that none of 13 judges who participated "requested the taking of a vote" on whether to rehear case. On Supreme Court, Justices Sandra O'Connor and Byron White voted to reconsider case. FCC's definition of indecency: "Language or material that depicts or describes, in terms patently offensive as measured by contemporary community standards . . . sexual or excretory activities or organs." Agency has fined several stations for indecent programming in the last year.

With loss in Supreme Court, FCC official told us "we don't have any choices left" but to permit such programming to be broadcast. "We're back to Act I." Source predicted, and other FCC officials agreed, that agency soon will issue rulemaking to make a ban on indecent programming later than 8 p.m. Same sources expect Congress once again to take up issue.

ACT President Peggy Charren said: "It's very exciting for ACT to have won one for the First Amendment. We always knew it's preposterous for the FCC to try to ban speech at 3 o'clock in the morning to protect children . . . It's very satisfying to have this particular [conservative] Supreme Court agree with us." NAB (which also was intervernor in case) Associate General Counsel Steve Bookshester said Supreme Court "correctly" acted in not reviewing lower court decision: "Now, it's up to the Commission to adopt new procedures to determine when such material is permitted to be broadcast." Washington attorney Timothy Dyk, who represented intervenors, said: "I think it's a very happy result . . . The Court of Appeals decision is exactly where it should be in terms of a safe harbor."

Drug Enforcement Data Are Vulnerable Through Phone Lines March 4, 1992
~~~~~~
Taken from Communications Daily (Page 5)

Classified information in computers of Drug Enforcement Administration (DEA) is at risk, General Accounting Office (GAO) said in a report. It said DEA doesn't provide adequate protection of classified information because too many people have access to computers that store data, and computers with classified information are hooked into nonsecure telephone lines, making them vulnerable to outside intrusion.

Report, Computer Security: DEA Is Not Adequately Protecting National Security Information (GAO/IMTEC-92-31), said it found several instances of lax physical and electronic security at DEA computers in several locations. Although there are no known instances of security breaches, "these disturbing security

weaknesses pose serious risks that could potentially hinder DEA's mission and threaten the lives of federal agents," the report said. The report found that DEA isn't complying with standard security guidelines outlined by National Security Agency.

In preliminary findings, GAO was so concerned with security weaknesses that it called in Department of Justice on January 9 and furnished it with a "limited official use" version of its report to give DEA time to correct problems, said Rep. Wise (D-W.Va.), chairman of House Government Operations Subcommittee, who ordered the investigation. He said other government agencies should be wary of sharing information with DEA until security problems have been eliminated. Calls to DEA on progress of follow-up security procedures weren't returned. Findings are "indicative" of typical "apathetic security attitude" that the government has, said David Banisar, security expert for Computer Professionals for Social Responsibility.

GAO investigators found DEA couldn't adequately identify what computers used classified information. "DEA cannot ensure that adequate safeguards are in place for protecting national security information," report said. In spite of federal guidelines, GAO found that DEA hasn't "completed a risk analysis" of computer system. Some classified computers were found to be operated in areas where contractors -- with no security clearances -- moved around with no restrictions. No computers were found to be "tempest" hardened, meaning electronic emissions from keyboards can't be picked up.

In light of concern on outside intrusion from "hackers," GAO found several DEA computers were connected by phone lines "that are not encrypted" -- which it described as clear violation of national security guidelines. The report said "unauthorized individuals can intercept or monitor information emanating from and transmitted by" the agency without being detected. Classified information was found to be stored on hard disks in an "inadvertent" manner, allowing for the possibility that computers, when resold, still might hold data. One such occurrence, recorded by GAO in its report, occurred last year when sensitive grand jury information on informants was left on surplus computers sold by DoJ at a public auction.

The report said that DEA has acknowledged weaknesses "and is taking action to correct them."

BBS Controversy Brews Close To Home March 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Taken from Puget Sound Computer User
Special Thanks: Peter Marshall in Telecom Digest

In a case before the Public Utility Commission of Oregon, US West is maintaining three phone lines connected to a free-access BBS in a residence should be billed at business rates. Because of the similarities in tariffs >from state to state and US West's position in the case, many are predicting that if US West prevails, the company will be authorized to raise all Oregon BBS lines to business rates and try to raise rates for BBS lines in US West's remaining 13 states.

The case started when Tony Wagner, a Portland system operator, received a letter from US West in October, 1991. In the letter, Communications Consultant Sandi Ouelette said "Bulletin board services are considered a business, therefore, subject to business rates ..."

One Seattle attorney interested in telecommunications said these attempts by the phone companies to raise rates for BBSes are "just another attempt to swipe people's communication."

1-800-54-PRIVACY March 10, 1992
~~~~~~~~~~~~~~~~

Taken from Communications Daily

American Newspaper Publishers Association (ANPA) President Cathleen Black asked American Paper Institute to support the newspaper industry's fight against RHCs, warning that the market for paper could drop if phone companies are

allowed to expand activities into information services. Increased electronic classified ads and other services could lead to cutbacks in demand for newsprint, Black said. Newspaper producers, traditionally allied with ANPA, said they would study the matter.

Meanwhile, full-page newspaper ads placed by ANPA and allied Consumer Federation, Graphic Communications International Union, National Newspaper Association, and Weatherline have generated thousands of calls to an 800 number >from readers concerned about potential invasions of privacy by telephone companies. The latest ad ran in the March 7 Washington Post, under the headline: "Unless they're stopped, the Bells will know more about you than even the IRS." The ad advised callers to dial 1-800-547-7482, referred to in the telephone message as "1-800-54-privacy."

Gary Slack, of the Chicago PR firm Slack, Brown & Myers, which is coordinating the 800 campaign, said that the angle in the ad has become an effective weapon against RHCs because "there are a lot of people concerned about privacy." Callers are sent a 4-page letter signed by Black and "action guidelines" for asking legislators to support bills by Representative Cooper (D-Tenn.) (HR-3515) and Senator Inouye (D-Hawaii) (S-2112) that would restrict RHC entry into information services. ANPA has argued that, through data on telephone bills, information can be collected about callers.

RHCs didn't have the incentive to use that data before, but now with the ability to offer information services, they do, ANPA said. ANPA generally doesn't pay for ads, but offers them to newspapers to run when they have space, a spokesman said. Pacific Telesis Vice-President Ronald Stowe said ANPA ads "show desperation and questionable ethics." He said ANPA is using some of same tactics it has accused RHCs of using, including collecting information on subscribers. ANPA ads are "really sewer-level stuff," Stowe said: "There are enough legitimate issues that ought to be debated."

*** Editor's Note: For more information on this story, please see "Standing Up To Fight The Bells" by Knight Lightning in this issue of Phrack.

- -

Missouri Bulletin Board Case Settled March 24, 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Taken from Communications Daily (Page 6)

Southwestern Bell in Missouri has filed a new tariff with the Missouri Public Service Commission (PSC) to allow computer bulletin board (BBS) operators to use residential lines. The tariff would take effect April 10 if there are no complications. Under proposal, the BBS operators at homes would be allowed to continue to use residence lines if they don't "solicit or require any remuneration, directly or indirectly, in exchange for access" and use 4 or fewer residential lines priced at flat rates.

BBSes that don't meet those requirements would be required to use business lines. The tariff, negotiated between SWB and representatives of BBS operators, defines a BBS as "a data calculating and storage device(s) utilized as a vehicle to facilitate the exchange of information through the use of Southwestern Bell Telephone Company facilities." BBS language is part of a high-grade Information Terminal Service originally aimed at business users with computers, but interpreted by BBS operators as targeted at them. SWB originally had wanted to make the new service mandatory for computers with modems, but the new proposal, submitted March 11, makes it optional.

*** Editor's Note: For more information, please see the numerous articles on this topic in Phrack World News, Issue 37, Part 3.

- -

In a surprising turn of events, the April 14, 1992 issue of Communications Daily reports that U.S. West in the state of Washington has decided not to follow the example of Oregon attempt to raise rates for electronic bulletin board (BBS) hobbyists.

Patsy Dutton, consumer affairs manager for Washington Utilities & Transportation Commission (WUTC), asked U.S. West about its policy after
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

receiving request from BBS operators.

In a letter dated March 31 to system operator Bruce Miller, Dutton said she had reviewed U.S. West tariff and had talked with company representatives as to current and future plans for BBS service: "The company indicates it has no intention of changing its current procedure." Residential service would be available for hobbyists, with business rates applying under other conditions.

An Oregon PUC law judge is currently considering complaint against U.S. West for raising rates of bulletin board operators there.

Congress Explores Dropping Subsidy of Federal Science Network March 13, 1992

Taken from Communications Daily (Page 6)

"Fairness For All Is Urged"

In hearing, Representative Boucher (D-Va.) questioned National Science Foundation (NSF) on its management policies and future direction of NSFnet, national research network. He said it's "essential" that NSFnet be structured so all commercial providers of network services "receive equal treatment" and that government policy for managing the network "not favor any provider" or set of providers.

The current process of using federal money to subsidize NSFnet is "obsolete" said Mitchell Kapor, representing Commercial Internet Exchange (CIX) Association, a consortium of commercial network services suppliers. Although federal money was necessary in the "early stages," when technology for building the network still was "experimental," now that the network is in place, government subsidy should stop, Kapor said. He said CIX members can provide "any level of service" needed by the same community served by NSFnet -- research and education. Kapor said CIX members could build and service national backbones with "off-the-shelf" technology; however, he said, because federal money goes to support the current network backbone, NSFnet users are allowed on the network free and don't have an incentive to use commercial services.

William Schrader, president of Performance Systems International (PSI), said government could level the playing field by providing money directly to individual universities and letting them choose, on a "free-market" basis, which network service provider to use. That system, he said, would provide incentive for several suppliers to upgrade networks in efforts to corral most customers. Kapor said it also would "push the envelope" of technology to an even greater level. With the current system in place, the technological level of the network will evolve more slowly because there would be no incentive to provide a higher level of service, he said.

Current users of NSFnet spoke against changing the status quo. Michael Roberts, VP-networking for Educom, a task force of 48 universities, said that removing funding for the network would be "horrendous." By requiring individual universities to seek out their own service providers, he said, government would have to institute another level of bureaucracy, creating "thousands of entitlements," which would be impossible logistically. Douglas Van Houweling, speaking for NSFnet manager Merit, said removal of funding most likely would upset the networks' level of stability, leading to disruption in service that "millions of users" have become accustomed to. By letting "any number" of commercial providers supply network services, there would be no guarantee of level of service, which is a "vital" mission of research labs, universities and federal agencies now using the network, Van Houweling said.

Federal agencies would rather have a stable network than improved service, said Stephen Wolff, director of NSF's Networking & Communications Division. He told Boucher that federal agencies didn't want the network open to competition because they feared it would degrade the quality of service. Wolff said NSF would proceed with its plan to commercialize network "within 5 years" as requested under the recently voted High-Performance Computing Act. He also said he had presented to universities the idea of providing them with federal money and letting them purchase network services in the free market. The proposal was "soundly rejected," he said, because universities didn't feel they

were able to make such decisions. Instead, they supported NSF's current proposal of rebidding network management so that 2 network providers would be in place. The new system would operate on model of government's FTS 2000 program. NSF would grant awards for network services to 2 companies and have an independent 3rd party act as "traffic manager" to ensure one network provider wasn't favored over another.

MCI and Sprint Take Steps To Cut Off Swindlers April 1, 1992

By Kent Gibbons (The Washington Times)(Page C1)

MCI and Sprint are cracking down on telephone fraud.

The two long-distance carriers are tackling different kinds of swindles, though:

* MCI said it will stop sending out bills for pay-per-call operators who promise help getting a loan, credit, a credit card or a job.

* Sprint said it will offer large business customers a form of liability insurance against unauthorized use of corporate switchboard lines.

MCI Communications Corporation of the District said it wanted to protect consumers who might be gulled into overpaying for some "900-number" services during economic troubles.

But long-distance carriers are also guarding their own bottom lines by tightening up pay-per-call standards, said telecommunications analyst James Ivers.

"They're acting fiscally responsibly because traditionally, these were the types of programs that created a high level of uncollectible" bills when ripped-off consumers refused to pay, said Mr. Ivers, senior analyst with Strategic Telemedia, a consulting firm in New York.

Last September, Sprint Corporation, of Kansas City, MO, told more than 90 percent of its 900-number customers it would no longer do their billing. Long-distance firms cannot refuse to carry pay-per-call services, but most 900-number operators do not want the expense and trouble of doing their own collections.

American Telephone & Telegraph Co., of New York, said it has set up strict guidelines for all 900-number firms, such as disclosing in advertising any fees charged for credit processing.

AT&T spokesman Bob Nersesian said: "We still think there are legitimate providers of this kind of service and our guidelines keep the dishonest guys off the network."

Sprint's switchboard-fraud liability protection is aimed at big customers, whose Sprint bills are more than $30,000 per month.

For an installation fee (up to $5,000) and a monthly charge (also up to $5,000), Sprint will absorb fraudulent phone charges above $25,000 per switchboard. The customer pays the first $25,000. Sprint's liability ends at $1 million.

Large and medium-sized companies can rack up huge bills if their private switches, known as private branch exchanges or PBXes, are broken into and used to make calls to other countries.

In a recent case, more than 20,000 calls were made on a company's PBX over a weekend, with the charges estimated at more than $1 million, said M.R. Snyder, executive director of Communications Fraud Control Association, a Washington trade group.

"It is certainly a fraud target that is ripe for being abused," Ms. Snyder said, especially since telephone carriers have improved their ability to spot unauthorized credit-card calls more quickly.

Overall, telecommunications fraud costs phone carriers and customers an estimated $1.2 billion per year, although the figure is really just a "guesstimate," Ms. Snyder said.

Company PBXes often have features that allow traveling employees, or distant customers, to call in and tap an outgoing line. With computer programs, hackers can randomly dial numbers until they hit security codes.

Sometimes the codes are only four digits, so hackers don't even need a computer, said Bob Fox, Sprint's assistant vice president of corporate security.

Along with the fees, customers must agree to take certain precautions. Those include using security codes at least eight digits long and eliminating the ability to tap outside lines through voice mail. In return, Sprint will also monitor PBX use every day, instead of the five days per week currently done free for customers, Mr. Fox said.

MCI spokesman John Houser said his company will be watching Sprint to see if the program is a success. Spokesman Andrew Myers said AT&T offers fraud protection to some corporate customers, but is not considering extending that to cover PBX abuse.

AT&T is currently involved in several lawsuits over disputed PBX charges that total "many millions" of dollars, Mr. Myers said. Sprint officials said they have not sued any customers to collect on PBX fraud bills.

Sprint Offers Liability Limit For Corporate Phone Fraud April 1, 1992

By Edmund L. Andrews (New York Times)(Page D4)

The Sprint Communications Company, the nation's third-largest long-distance carrier, said that it would limit the liability of large corporate customers for the huge bills rung up by phone-service thieves who manipulate a company's telephone switching equipment and voice-mail systems.

Typically, such thieves call into a company on one of its toll-free "800" numbers and then figure out the codes necessary to obtain an outgoing line that can be used to call anywhere in the world. These telephone "hackers" often sell plundered telephone codes to illegal operators who then sell overseas calls to hundreds of people at a time. Sprint officials said this sort of fraud approached $1 billion a year.

The new Sprint plan would be available to companies that signed two-year contracts to buy at least $30,000 of international long-distance service a month and agreed to adopt a series of protective measures. These include installing longer telephone codes that are harder for thieves to crack and new limits on the ability of voice-mail systems to obtain outgoing lines.

In exchange, customers would be held responsible for no more than $25,000 in stolen calls for each round of break-ins, and a maximum limit of $1 million a year. Although that is still a substantial sum, it is much less than many companies have lost in recent years from theft of service by telephone hackers.

A Point of Contention

Thieves broke into the switchboard of Mitsubishi International in New York in 1990, for example, and ran up $430,000 in overseas telephone calls. Procter & Gamble lost $300,000 in a similar incident in 1988. Had either company been operating under the new Sprint plan, its liability would have been limited to $25,000.

Long-distance carriers and their corporate customers have long argued over who should bear responsibility for the huge bills caused by service theft. The carriers have maintained that their customers are responsible for these bills, even if fraud is undisputed, arguing that the thieves took advantage of weaknesses in the customers' equipment, rather than in the weaknesses of the long-distance network itself.

But some corporate victims have argued that they had no idea their systems were vulnerable, while others contend that they incurred big losses even after adopting special security procedures.

MCI Moves Against ’900’ Fraud

In a separate issue involving telephone fraud, MCI Communications Corporation said it would no longer provide billing services for companies that use "900" numbers to offer credit cards, and that it would place tough new restrictions on the use of 900 numbers to sell job-placement services, contests and sweepstakes.

The long-distance company said its decision was based on numerous complaints about abusive and fraudulent sales practices. Companies that provide information through the use of telephone numbers with the 900 area code charge callers a fee each time they call the number. MCI and other long-distance companies carry these calls and bill customers on behalf of the company that provides the information service.

Pam Small, an MCI spokeswoman, declined to say how much revenue the company would lose because of the suspension. But she said the 900 services that would be affected represented a small part of its pay-per-call business.

==Phrack Inc.==

Volume Four, Issue Thirty-Eight, File 15 of 15

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN     Issue XXXVIII / Part Three of Three     PWN
PWN                                             PWN
PWN        Compiled by Dispater & Friends       PWN
PWN                                             PWN
PWN     Special Thanks to Datastream Cowboy     PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

CFP-2: Sterling Speaks For "The Unspeakable" March 25, 1992

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

WASHINGTON, D.C. -- Bruce Sterling, the prime luncheon speaker at the 2nd Annual Conference On Computers Freedom & Privacy (CFP-2), fulfilled his program billing as "Speaking for the Unspeakable" by taking on three separate persona and delivering what might have been their messages.

Sterling, best known as a science fiction writer, spoke for three characters, a "a malicious hacker," a Latin American police official, and a Hong Kong businessman, who were, in his words, "too venal, violent, treacherous, power-mad, suspicious, or meanspirited to receive (or accept) an invitation to attend."

Sterling began his speech by introducing himself and then saying, "When the CFP committee asked me if I might recommend someone to speak here at CFP-2, I had an immediate candidate. I thought it would be great if we could all hear from a guy who's been known as Sergei. Sergei was the KGB agent runner for the Chaos Computer Club group who broke into Cliff Stoll's computer in the famous Cuckoo's Egg case. Now Sergei is described as a stocky bearded Russian espionage professional in his mid-40s. He's married, has kids and his hobby is fishing, in more senses than one, apparently. Sergei used to operate out of East Berlin, and, as far as I personally know, Sergei's operation was the world's first and only actual no-kidding, real-life case of international computer espionage. So I figured -- why not send Yelsin a fax and offer Sergei some hard currency; things are pretty lean over at KGB First Directorate these days. CFP could have flown this guy in from Moscow on a travel scholarship and I'm sure that a speech from Sergei would be far more interesting than anything I'm likely to offer here. My proposal wasn't taken up and instead I was asked to speak here myself. Too bad!

"This struck me as rather a bad precedent for CFP which has struggled hard to maintain a broad universality of taste. Whereas you're apparently willing to tolerate science fiction writers, but already certain members of the computer community, KGB agents, are being quietly placed beyond the pale. But you know, ladies and gentlemen, just because you ignore someone doesn't mean that person ceases to exist -- and you've not converted someone's beliefs merely because you won't listen. But instead of Comrade Sergei, here I am -- and I am a science fiction writer and, because of that, I rejoice in a complete lack of any kind of creditability!

"Today I hope to make the best of that anomalous position. Like other kinds of court jesters, science fiction writers are sometimes allowed to speak certain kinds of unspeakable truth, if only an apparent parody or metaphor. So today, ladies and gentlemen, I will exercise my inalienable civil rights as a science fiction writer to speak up on behalf of the excluded and the incredible. In fact, I plan to abuse my talents as a writer of fiction to actually recreate some of these excluded, incredible unspeakable people for you and to have them address you today. I want these people, three of them, to each briefly address this group just as if they were legitimately invited here and just as if they could truly speak their mind right here in public without being arrested."

Sterling then went on to assure the crowd that he was not speaking his personal conviction, only those of his characters, and warned the group that some of the material might be offensive. He then launched into the delivery of his characters' speeches -- speeches which had the hacker talking about real damage -- "the derailing of trains"; the Latin police official, a friend and admirer of Noriega, discussing the proper way of dealing with hackers; and the businessman explaining way, in the age of high speed copiers, laser printers and diskette copying devices, the US copyright laws are irrelevant.

Often intercepted by laughter and applause, Sterling received a standing ovation at the conclusion of the speech. Computer Press Association newsletter editor Barbara McMullen was overhead telling Sterling that he had replaced "Alan Kay as her favorite luncheon speaker," while conference chair Lance Hoffman, who had received an advance copy of the speech a few weeks before, described the speech as "incredible and tremendous".

Sterling, relaxing after the talk with a glass of Jack Daniels, told Newsbytes that the speech had been fun but a strain, adding, "Next time they'll really have to get Sergei. I'm going back to fiction."

Sterling's non-fiction work on computer crime, "The Hacker Crackdown" is due out from Bantam in the fall and an audio tape of the CFP-2 speech is available >from Audio Archives. He is the author of "Islands In The Net" and is the co-author, with William Gibson, of the presently best-selling "The Difference Engine."

- -

The Bruce Sterling luncheon video tape is now available, sizzling, and affordable to the Phrack readers.

$19.95 + $4 (shipping and handling)

Call now: (800)235-4922
or
CFP Video Library Project
P.O. Box 912
Topanga, CA 90290

Tell them you heard about it from The WELL and you'll get the above price.

CFP-2 Features Role-Playing FBI Scenario March 25, 1992
~~~~~~

By Barbara E. McMullen (Newsbytes)

WASHINGTON, D.C.-- As part of the "Birds-of-a-Feather" (BOF) sessions featured at the 2nd Conference on Computers, Freedom & Privacy (CFP-2), FBI Agent J. Michael Gibbons, acting as a live gamemaster, orchestrated the play-acting of an investigation by federal agents into allegations of computer intrusion and criminal activity.

The scenario, set up by Gibbons to show the difficulties faced by investigators in balancing the conducting of an investigation with a protection of the rights of the individual under investigation, was acted out with non-law enforcement officials cast in the role of investigators; New York State Police Senior Investigator Donald Delaney as "Doctor Doom," the suspected ringleader of the computer criminals; Newsbytes New York Bureau Chief John McMullen as a magistrate responsible for considering the investigators' request for a search warrant; and author Bruce Sterling as a neighbor and possible cohort of Doctor Doom.

Gibbons, in his role of Gamemaster, regularly intercepted the action to involve the audience in a discussion of what the appropriate next step in the scenario would be -- "Do you visit the suspect or get a search warrant or visit his school or employer to obtain more information? Do you take books in the search and seizure? Printers? Monitors? etc." During the discussion with the audience, points of law were clarified by Mike Godwin, Electronic Frontier Foundation in-house counsel, and Alameda County Assistant District Attorney Donald Ingraham.
~~~~~~

The role-playing session immediately followed a BOF panel, "Hackers: Why Don't They Understand" which attempted to present a hacker view of on-line ethics. The panel, moderated by McMullen, was composed of Steven Levy, MacWorld columnist and author of "Hackers"; Dorothy Denning, Chair of Computer Science at Georgetown University; Glenn Tenney, California Congressional candidate and chair of the annual "Hacker's Conference"; Craig Neidorf, defendant in a controversial case involving the electronic publishing of a stolen document; "Dispater," the publisher of the electronic publication "Phrack"; Emmanuel Goldstein, editor and publisher of "2600: The Hacker Quarterly," and hacker "Phiber Optik."

During the panel discussion, Levy, Denning and Tenney discussed the roots of the activities that we now refer to as hacking, Goldstein and Dispater described what they understood as hacking and asked for an end to what they see as overreaction by the law enforcement community, Neidorf discussed the case which, although dropped by the government, has left him over $50,000 in debt; and Phiber Optik described the details of two searches and seizures of his computer equipment and his 1991 arrest by Delaney.

In Neidorf's talk, he called attention to the methods used in valuing the stolen document that he published as $78,000. He said that it came out after the trial that the $78,000 included the full value of the laser printer on which it was printed, the cost of the word processing system used in its production and the cost of the workstation on which it was entered. Neidorf's claims were substantiated by EFF counsel Godwin, whose filing of a motion in the Steve Jackson cases caused the release of papers including the one referred to by Neidorf. Godwin also pointed out that it was the disclosure by interested party John Nagle that the document, valued at $78,000, was obtainable in a book priced at under $20.00 that led to the dropping of the charges by the US Attorney's office.

SRI security consultant Donn Parker, one of the many in the audience to participate, admonished Phiber and other hackers to use their demonstrated talents constructively and to complete an education that will prepare them for employment in the computer industry. Another audience member, Charles Conn, described his feeling of exhilaration when, as a 12-year old, he "hacked" into a computer at a local Kentucky Fried Chicken. Conn said "It was wonderful. It was like a drug. I just wanted to explore more and more."

Parker later told Newsbytes that he thought that it was a mistake to put hackers such as Phiber Optik and those like Craig Neidorf who glorify hackers on a panel. Parker said, "Putting them on a panel glorifies them to other hackers and makes the problem worse."

The Birds-of-a-Feather sessions were designed to provide an opportunity for discussions of topics that were not a part of the formal CFP-2 program.

Computer Revenge A Growing Threat March 9, 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

By Tom Steinert-Threlkeld (Dallas Morning News)
Article in the Chicago Tribune, Page C3

The "downsizing" of corporate America is not only making companies lean and mean.

It's doing the same thing to employees losing their jobs, said Thomas F. Ellis, a partner in Arthur Andersen & Co.'s Computer Risk Management Services.

He looks at the latest form of revenge by employee against former employer. Fraud, embezzlement and theft of secrets are no longer the only forms of frustrated payback. The calling card in the digital age is computer sabotage.

It's an invisible epidemic that corporations don't like to talk about while they're trying to convince banks and creditors they are becoming more efficient by downsizing, said Ellis and William Hugh Murray, information systems security consultant to Deloitte & Touche, another of the Big Six accounting firms.

"A lot of the business trends in the U.S. are really threatening data
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

security," said Sanford M. Sherizen, a Natick, Massachusetts computer security consultant. "Corporations are paying a huge price for it," without disclosing it.

The downsizing has led to inadequate attention to security precautions, argues Sherizen. The underlying trend: Fewer and fewer people are being given more and more responsibility for information systems.

That breeds opportunity for revenge, said Sherizen. No longer does only the supposedly misfit hacker, gulping down Cokes and Fritos in the middle of the night, merit watching. Sherizen's worldwide set of clients have found that the middle manager wearing the white shirt and tie in the middle of the day also deserves scrutiny, he says.

Those managers, if mistreated, find it inviting to strike back creatively. The VTOC, for example.

This is jargon for the Volume Table of Contents. This is a directory a computer compiles to keep track of where programs and data are stored. A large Andersen client was paralyzed recently when a VTOC in its information system was scrambled by a downsizing victim, Ellis said.

"If you destroy the VTOC in a mainframe system, then you destroy the computer's ability to go out and find programs and data, so you can pretty effectively devastate a computer installation by destroying the VTOC, without ever touching the programs and data," he said.

But those bent on revenge are not above leaving time bombs in computer systems that will go off after their departure, destroying programs and data.

They also are appropriating information from magnetic memories and selling it at hefty prices in the burgeoning field known euphemistically as "commercial business intelligence," said Sherizen.

Most companies hush up these cases, because they fear copycat avengers will strike when their vulnerability is exposed. They also don't like to be publicly embarrassed, the security experts say.

Technical safeguards don't hold a candle to human safeguards, said Murray.

The best way to protect against sabotage is to prevent disaffection in the first place. Treat as well as possible those who are being fired. Compensate fairly those who are staying.

Show appreciation, day in and day out. Most revenge is slow to boil and comes >from employees who finally conclude that their contributions are going unrecognized, said Murray.

"Saying 'please' and 'thank you' are an incredibly important control" against sabotage, he said.

Computer Crime Problem Highlighted March 9, 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

By Oscar Rojo (Toronto Star)(Page B3)

With the growing corporate dependence on computers, "information crimes" have become easier to commit but harder to detect, says a Toronto-based security company.

"Electronic intrusion is probably the most serious threat to companies that rely on computerized information systems," Intercon Security Ltd. says in its Allpoints publication.

Allpoints cited a study of 900 businesses and law enforcement agencies in Florida showing that one of four businesses had been the victim of some form of computer crime.

"While most of the media attention has focused on "hackers," individuals who deliberately and maliciously try to disrupt business and government systems,
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

one estimate indicates that 75 per cent plus of electronic intrusion crimes may be "insider attacks" by disgruntled employees," the publication said.

In Intercon's experience, vice-president Richard Chenoweth said the company is as likely to find a corporate crime committed by a disgruntled employee as one perpetrated by an outsider.

Intercon said the technology exists to guard against most electronic intrusions. "The problem is that many information managers still don't believe there is a risk, so they are not making the best possible use of what is available."

Criminals Move Into Cyberspace April 3, 1992

By Mick Hurrell (The Times)(Features Section)

The hacker and the virus programmer embodied the popular notion of computer crime in the 1980s, and they are still the most widely known criminal acts in computer technology.

The advent of new technologies over the past decade has created a whole new casebook of serious crimes, but they have yet to gain the notoriety of computer viruses such as Friday 13th or Michelangelo.

More then 3,000 computer crimes around the world in the past 20 years have now been documented by SRI International (SRII), a Californian information security consultancy. They include attempted murder, fraud, theft, sabotage, espionage, extortion, conspiracy and ransom collection.

Against this disturbing background, Donn Parker, SRII's senior international security consultant, is telling businesses they will be under increasing attack >from sophisticated criminals using computer technology and from others intent on causing disruption.

"New technology brings new opportunities for crime," he says. "We must anticipate future types of crime in our security efforts before they become serious problems."

His prospective list ranges from the annoying to the fraudulent, and includes small computer theft, desktop forgery, digital imaging piracy, voice and electronic mail terrorism, fax graffiti attacks, electronic data interchange fraud, and placement of unauthorized equipment in networks.

Some of these crimes are more obvious than others. The advanced digital imaging systems now being used in the television and film industry to create spectacular special effects, for example, could become a new target for crime. As digital imaging can alter video images seamlessly, the possibilities for sophisticated fraud are numerous.

The theft of small computers and components has already increased. "I think it will be worse than the typewriter theft problem of the 1970s and 1980s," Mr. Parker says. "We are now teaching information-security people that they have to learn how to protect small objects of high value. The content of the computers could be more valuable than the hardware itself.

"I do not think the criminal community is yet aware of a computer's value other than on the used equipment market, but ultimately some are going to figure out that the contents the data are more valuable, which could lead to information being used for extortion."

Desktop forgery is another crime that looks certain to boom and plague businesses of all types. Desktop publishing software, combined with the latest color laser printers and photocopiers, is proving an ideal forger's tool. Gone is the dingy cellar with printing plates and press: Forgers can work from comfortable offices or their own homes and produce more accurate fakes than ever before.

Original documents can be fed into a computer using a scanner, then subtly altered before being printed out. Business documents such as purchase orders

and invoices are obvious targets for the forgers, as are checks. The quality of a forgery is now limited only by the paper on which it is printed.

Mr. Parker says: "As the technology gets cheaper and more available, this is something that could flourish."

But although many of these new forms of computer crime bring with them the possibility of increased business losses, one threat overshadows them all. "The big security issues are going to involve networks and the connection of computers to many others outside an organization," says Rod Perry, a partner with Coopers & Lybrand Deloitte, the consultants.

The fear is that sophisticated criminals will take advantage of a clash between the desire for system flexibility and the constraint necessarily imposed by security. Mr. Perry adds: "The business need is paramount, and people will accept the risk up to a point."

Networks are attractive because they allow information to be easily transferred between users, and give free and easy access to data bases from many locations within an organization that can extend across countries and continents. Making them secure against interference from both outside and within is difficult.

Mr. Parker says: "Today's microcomputers and local and global networks have left information security far behind. We are dealing with what we call cyberspace. We are connecting our networks so that we now have a single worldwide network of data communications.

"We have inadvertently freed the criminal from proximity to the crime. A criminal can be anywhere in the world, enter cyberspace by computer, and commit a crime anywhere else. The criminal is free to choose the jurisdiction area >from which he works, to minimize the punishment if he gets caught."

The great concern, he says, is if technological advances result in an "anarchy of conflicting security efforts. Consistent security practices should be applied uniformly as well as globally.

"When organizations in different countries with different national laws, different ways of valuing information assets, and different national ethical customs, use equipment from different manufacturers in their networks, they face the problem of matching their levels of security. They use the lowest common denominator, which in some instances may be practically non-existent."

Some computer security consultants believe that network security headaches will involve some restriction in how they are used. All agree that passwords no longer offer appropriate forms of security.

Professor Roger Needham, of the University of Cambridge computing laboratory, says: "At the moment, there is a lot of shoddy computer use, but it will become more usual to take security seriously. In the world of doing business with paper, there are a tremendous number of rules of practice and conduct that are second nature; security procedures in the electronic medium will also have to become second nature."

SRII is developing software for what it says will be the world's most sophisticated detection system, designed to identify criminal users as they commit their crime.

Called IDES (Intruder Detection using Expert Systems), it works on the basis that a system intruder is likely to show a different behavior pattern from that of a legitimate user. IDES is programmed with a set of algorithms that build up profiles of how particular employees typically use the system. It can then inform the company's security division if it identifies any significant deviation.

IDES also monitors the whole system for failed log-in attempts and the amount of processor time being used, and compares this with historical averages.

A future refinement will allow the system to profile groups of subjects so that it can tell, for example, when a secretary is not behaving like a "typical" secretary.

Business crime and computer crime will increasingly become one and the same, Mr. Parker says. Security will be increasingly built in to systems and "transparent" to the user.

"I think the overall loss to business from computer crime will decrease," he says. "But the loss per incident will increase because the risks and the potential gains will be greater."

PWN QuickNotes
~~~~~~~~~~~~~~

1. New Law Enforcement Bulletin Board (Government Technology, January 1992, Page 17) -- St. Paul, Minnesota -- The International Association of Chiefs of Police (IACP) and LOGIN Information Services has announced IACP NET, a new computer network that will link law enforcement professionals nationwide. The network uses advanced computer capabilities to foster and empower IACP's belief that strength through cooperation is the key to the success of law enforcement endeavors.

   Communications services will be the interaction focus. An electronic mail feature allows private messaging among IACP NET members. Exchange of ideas will be encouraged and facilitated through electronic bulletin boards on general subject areas and computer conferencing on specific topics. Anchoring the communications service is the Quest-Response Service, a service created and proven successful by LOGIN that allows members to post and respond to requests for information in a formatted and accessible manner.

---

2. ATMs Gobble Bankcards In Colorado (Denver Post, February 19, 1992) -- About 1,000 Colorado ATM users had their Visas and Mastercards abruptly terminated in February by an out-of-control computer system.

   For 90 minutes during the President's Day weekend, the Rocky Mountain Bankcard System software told ATMS around the state to eat the cards instead of dishing out cash or taking deposits. The "once-in-a-decade" glitch went unnoticed because it occurred as programmers were patching in a correction to a different problem.

   The company is rushing new plastic and letters of apology to customers who got terminated.

---

3. Minister Denies Hackers Tampered With Licence Records (Chris Moncrieff, Press Association, January 27, 1992) -- Allegations that computer experts hacked into the records of the Driver and Vehicle Licensing Agency in Swansea are without substance and are to be retracted, Roads and Traffic Minister Christopher Chope said.

   He was responding in a Commons-written reply to Donald Anderson (Lab Swansea East), who had asked what investigations had been made following a report that hackers had been able to erase driving convictions from DVLA computer files. Mr. Chope said, "The Agency has discussed the recent allegations about unauthorized access to its computer records with the author of the original Police Review article, who has confirmed that there is no substance to them. "The author has agreed to retract the allegations in his next article." Mr. Anderson commented, "The importance of this reply is that it underlines the integrity of the system of driver-licence records held in Swansea in spite of the allegations."

---

4. Software Virus Found At INTEL (New York Times News Service, March 3, 1992) -- Intel Corporation said it had stopped shipping a computer network software program because some units were found to be infected with the "Michelangelo" virus, a program that infects IBM and compatible personal computers and can potentially destroy data.

   A division of Intel in Hillsboro, Oregon, said it had shipped more than 800 copies of the program, called LANSpool 3.01, which inadvertently contained
~~~~~~~~~~~~~~

the virus. The virus is designed to activate on March 6, Michelangelo's birthday, and can erase data and programs if it is not detected with antiviral software.

The company said it had checked its software with a virus-scanning program before shipping it, but that it had failed to detect the virus.

A number of computer makers and software publishers have issued similar alerts about the Michelangelo program and a variety of companies are now offering free software to check for the virus.

There are more than 1,000 known software viruses that can copy themselves from computer to computer by attaching to programs and files.

---

5. Army Wants Virii (Bulletin of the Atomic Scientists, December 1991, Page 5)

"Attention Hackers, Uncle Sam Wants You!"

The U.S. Army has caught the computer virus bug and is now expanding its interest in germ warfare to include electronic germs.

The Army Center for Signal Warfare is soliciting proposals for the development of a "weaponized virus" or a piece of "malicious software" that could destroy an enemy's computers or software (_Technology Review_, October 1991). As project engineer Bob Hein explained, "This is the army. We're in the weapons business."

Hein said the army first became interested in the potential of computer viruses as offensive weapons after Myron Cramer's 1989 article in _Defense Electronics_ suggested that computer viruses offered "a new class of electronic warfare." But Gary Chapman, director of Computer Professionals for Social Responsibility, thinks it is more likely that the army's interest was piqued by a French science fiction novel, _Soft War_, describing army infiltration of Soviet computers.

Chapman, who called that army's plan to design killer computer viruses a "stupid policy," said that any viruses the army comes up with are more likely to paralyze the heavily networked U.S. computer system than to infiltrate enemy computers.

Hein insisted that the army will develop only controllable and predictable bugs that will not threaten U.S. computer users. Chapman pointed out that, like the biological agents they are named for, computer viruses are, by their very nature, uncontrollable.

---

6. BellSouth's MobilComm and Swiss watchmaker Swatch said they will form joint venture to market wristwatch pager. The watch will cost about $200 and will be sold in department stores. It will bear name of "Piepser," the German word for "beeper," using 4 tones to signal the wearer. Each signal is activated by a telephone number that owner assigns. In the 4th quarter of year, Swatch said it plans to introduce a model that can display telephone numbers. (Source: Communications Daily, March 5, 1992, Page 4)

---

7. U.S. District Judge Harold Greene denied several new motions by Nynex in a criminal case being brought by the Justice Department, charging the phone company with violating MFJ (Modified Final Judgment) through subsidiary Telco Research. The government also filed a new motion of its own, later denied, requesting Greene to hold a pretrial hearing to look into "actual or potential conflicts of interest" resulting from individuals to be called as witnesses for prosecution being represented by Nynex's law firm, Davis, Polk & Wardwell. DoJ said: "It appears that Davis, Polk represents present and former employes of Nynex in addition to the corporation." Nynex issued a statement saying it's "confident" that the trial would "confirm to our customers," shareholders, and the public that it has fully met its responsibilities under MFJ. Greene, having dismissed Nynex motions, set an April 6 trial date. (Communications Daily, March 24, 1992, Page 5)

---

8. US West has formed a subsidiary, US West Enhanced Services, that launched its first product, Fax Mail. The subsidiary will develop other products for the enhanced-services market, including voice, fax and data applications, the company said. Test marketing of Fax Mail was conducted in Boise and was product-introduced in Denver. US West described its new product as "voice mail for faxes," in that it stores incoming faxes until the subscriber calls in and instructs the service to print the waiting fax. Each fax mail subscriber is supplied with a personal fax telephone number. When a fax is received, Fax Mail can notify the subscriber automatically by depositing a message in voice mail or beeping a pager. The service costs $19.95 per month, US West said. (Communications Daily, March 24, 1992, Page 6)

---

9. Hacker Insurance -- Worried about the integrity of your bank's data network? Relax. Commercial banks and other depository institutions can now obtain up to $50 million in coverage for losses due to computer-related crime. A new policy from Aetna Casualty and Surety Co. offers insurance against computer viruses, software piracy, and toll-call fraud, among other high-tech rip-offs. The Hartford, Connecticut insurer will also cover liabilities due to service bureau and communications failures with Aetna Coverage for Computer and Electronic Network Technology. Paul A. Healy, VP of Aetna's fidelity bond unit, says "the policy will help institutions manage the risk associated with the changing technology." (Information Week, March 30, 1992, Page 16)

==Phrack Inc.==

Volume Four, Issue Thirty-Eight, File 2 of 15

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

By Phrack Staff

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

Terminus Is Free

Len Rose has been released from prison as of March 23, 1992. Those wishing to write him and send him U.S. mail:

Len Rose
Salvation Army Freedom Center
105 Ashland
Chicago, Illinois 60607

He will remain at this address until May 23, 1992.

Date: March 4, 1992
From: Sarlo
To: Phrack Staff
Subject: Loopback Correction

While scanning the loopback section of Issue 37, I came across this letter:

>:: Fed Proof Your BBS, NOT! ::
>
> I'm sure many of you have seen text files on making your BBS more secure.
>One such file floating around is by Babbs Boy of Midnight Society. One of the
>members of our Phrack Staff showed this document to EFF's Mike Godwin, who is
>an attorney. He had the following comments:

>- -
>
>From: Mike Godwin
>To: Phrack Inc.
>
>(In regards to some of the files about how to "fed-proof" your BBS:)
>
>> Let's start with the log on screen: If FEDZ want anything from your board,
>> they are required to provide 100% accurate information.
>
>This is false. Ask the legislators who've been convicted in "sting"
>operations. In fact, so far as I can tell in a brief run-through of this
>document, absolutely no part of the so-called "legal" advice is true.
>
>Law enforcement agents who misrepresent their identities (e.g., "undercover
>agents") produce admissible evidence all the time.
>
>--Mike

Allow me to clear some things up. Babbs' Boy was a friend of mine a while back and was more of a Game Programmer than a "hacker" (or "cracker," if you want to be anal about it). Babbs' Boy was NEVER in MsU. He had asked me if he could write a file for the group. We informed him that he could if he wanted to, but he could in no way represent us. According to Babbs' Boy, he retrieved the information from a copy of the ECPA. Since we were not releasing that as a MsU file, we never bothered to check any of the said information out. In fact, MsU does not create files for public display, although individual members may.

Apparently Babbs' Boy uploaded his copy of the document to Ripco, in which it went wideband from there. I am told that 3 other documents were released in MSU's name, by someone using one of my very old handles of Raistlin. I can assure you that these documents were not released by any legitimate (old or current) member of Midnight Society Underground.

Again, to clear things up, Babbs' is not nor ever was a member of MsU, nor are there any legitimate public releases from our group.

Besides, we don't let people in the group who spell Feds "FEDZ" ..the shit just ain't done.

Sarlo of Midnight Society Underground [MsU]

sarlo@gagme.chi.il.us

Date: March 22, 1992
From: "Michael E. Marotta" <MERCURY@lcc.edu>
Subject: Censorship in Cyberspace
To: Phrack Staff

I have been hired to write an article about the control of information in cyberspace. We all know that Fidonet moderators and sysops devote their OWN resources for us to use. There is no question about the "right" of the sysop or moderator to delete messages and users. The practice of censorship is nonetheless newsworthy.

If YOU have experienced censorship on Fidonet or Usenet, Prodigy or CompuServe, or another BBS or network, I am interested in learning about your story. If you can supply downloads of actual encounters, so much the better.

If you have ever been censored, send me physical world mail about the event.

Michael E. Marotta
5751 Richwood #34
Lansing, Mich. 48911

Dear Phrack Staff,

There are very serious negative consequences surrounding the use of modems and computers in our society. Because of this, all children under the age of 18 should be prohibited from using a computer in connection with a modem or that is connected to any computer service.

Please read my attached news release and join me in spreading this message.

-- Ron Hults

- -

NEWS RELEASE March 18, 1992

PEDOPHILIA, COMPUTERS, AND CHILDREN

If you have children in your home and a home computer complete with a telephone modem, your child is in potential danger of coming in contact with deviant and dangerous criminals.

Using the computer modem, these unsavory individuals can communicate directly with your child without your knowledge. Just as importantly, you should be concerned if your child has a friendship with other youth who has access to this equipment in an unsupervised environment.

Using a computer and a modem, your child can readily access community "bulletin boards" and receive sexually explicit and graphic material from total strangers who can converse with your children, individuals you quite probably wouldn't

even talk with.

The concern becomes more poignant when stated otherwise; would you let a child molester, murderer, or convicted criminal into your home to meet alone with your child?

According to Fresno Police Detective Frank Clark, "your child can be in real danger from pedophiles, rapists, satanic cultists and other criminals known to be actively engaged in computer conversation. Unwittingly, naive children with a natural curiosity can be victimized; emerging healthy sexual feelings of a child can be subverted into a twisted, unnatural fetish affecting youth during a vulnerable time in their lives."

It is anticipated that parents, when armed with the knowledge that this activity exists and awareness that encounters with such deviant individuals can result in emotional and psychological damage to their child, will take appropriate measures to eliminate the possibility of strangers interacting with their children via a computer.

For Further Information, contact Ron Hults (209)498-4568

Date: March 30, 1992
From: Anonymous
To: Knight Lightning <kl@stormking.com>
Subject: Thanks

Dear Knight Lightning,

I would like to thank you for the message you wrote to Dale (scumbag) Drew. Although the fact is that he will only be slightly inconvenienced by having to dig up issues of Phrack on his own instead of having them delivered to his mailbox, his being refused to be added to the mailing list means a lot more. If I were him, I would consider it a slap in the face (since it seems almost as bad, IMO, as being blacklisted). :)

May he run into 10 homosexual wrestlers in a dark alley.

Review of Intertek Winter 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

325 Ellwood Beach, #3
Goleta, CA 93117
Internet: steve@cs.ucsb.edu
Phone: 805-685-6557

Subscription Rates:
US : 4 issues (2 year) $14.00.
OS : 4 issues (2 year) $18.20.
Back issues : $5.00 ea.

by Dispater

Intertek is the *SHARPEST* looking 'zine I've seen yet that directly addresses the world of cyberspace. It's not "high res" color or artsy-fartsy like Mondo 2000, but it is at least more interesting to read as a whole. I think it looks better and is more direct and to the point. You don't have to wade through a bunch of trash to get to something interresting.

This issue of Intertek focused on "virtual communities." The topics included: "Bury USENET," "Electropolis (IRC)," "Social Organization of the Computer Underground" by Gordon Meyer, "Real World Kerberos," and "Mudding: Social Phenomena in Text-Based Virtual Realities." Every issue also contains the top news tidbits about some truly high-tech achievements that go unnoticed by the mainstream media (I guess the Mike Tyson trial gets more ratings, huh?). All in all, it was much more interesting to me than the last issue (Volume 3.2). It's magazines like this that I hope will help make the mainstream media obsolete.

If you are looking for "how-to" techie projects or hacking tips, this is NOT for you! Many hackers I know don't like it and think it's boring as hell; 2600 and Phrack it isn't. However, if you are interested in the "big picture" of the cyberspace (what ever that means! :) or are, say, interested in studying cyberspace from an uninvolved level, this is the magazine for you. Intertek is full of social insight into what makes the cyberspace tick. It does this much
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

better than the feeble attempts other magazines have made. For only $7.00 a year, I think it's worth it.

Hacking in Australia

By The Cure

Australia has been very sparse after my BBS (Micromation) was closed down. A lot of people took it as a warning, and closed up shop as well. The Amiga warez BBSes still continue to flourish, as do some IBM ones. Because of the expense of phone lines ($300 installation of a line, $250 per year rental [in American dollars]) we tend to have a lot of BBSes that are dual purpose, i.e. both warez and phreak. Devastation Phase One is a great example: huge Amiga/IBM/phreak/etc. I, however, was devoted to phreak/hack/etc. We did have a few busts actually, and the police were called in to trace all calls through Vicnet and some people I know were caught. We've got a few warez-monger type people here that have been busted for "pitting" (climbing into telecom phone pits, and hooking up straight to the lines) - and I had my knuckles rapped by my university. Phoenix's court case still hasn't been settled (he's had 35 of the 47 charges against him dropped). Comserve has finally made it down under, and they're footing the bill for the first year, allowing us to be on Comserve in the States for a while. Our telephone company (Telecom) is a government monopoly, and we've only just passed legislation to allow competition. The first carrier allowed will be a company called Optus. Call waiting, conferencing, etc. is almost standard here now.

Censorship in Iowa

From: Mike Begley <spam@iastate.edu>

Hi. I got your name from Erik Bloodaxe. He said you might be able to help us out with a minor problem we're having here. The computation center at Iowa State University will very soon institute a policy of censorship of a number of groups of questionable nature, specifically the alt.sex hierarchy, alt.drugs, and a few other similar groups.

I wish to conduct a survey of the users of our computer system, but the university specificly prohibits mass mailings.

I'm frightened by censorship, and I want to fight this as best I can. If you would be able to do this favor for us, you would be helping to fight electronic censorship and suppression of free expression.

Phrack FTP Sites

quartz.rutgers.edu (128.6.60.6)
Location: /pub/computer/law

mc.lcs.mit.edu (18.26.0.179)
Location: /its/ai/digex

mintaka.lcs.mit.edu (18.26.0.36)
Location: /telecom-archives

coombs.anu.edu.au (130.56.96.2)
Location: /inbound

wuarchive.wustl.edu (128.252.135.4)
Location: /doc/policy/pub/cud/Phrack

ftp.eff.org (192.88.144.4)
Location: /pub/cud/Phrack

nic.funet.fi (128.214.6.100)
Location: /pub/doc/phrack

cs.dal.ca (129.173.4.5)
Location: /pub/comp.archives

chsun1.spc.uchicago.edu (128.135.46.7)
Location: /pub/cud/phrack

ftp.uu.net (137.39.1.9)
Location: /tmp

rascal.ics.utexas.edu (128.83.138.20)
Location: /misc/ra/sa/ULM.DE

relay.cs.toronto.edu (128.100.3.6)
Location: /doc/telecom-archives

aix370.rrz.uni-koeln.de (134.95.132.2)
Location: /pub/usenet/comp.archives/hackers/journals

titania.mathematik.uni-ulm.de (134.60.66.21)
Location: /info

src.doc.ic.ac.uk (146.169.3.7)
Location: /usenet/comp.archives/hackers/journals

bric-a-brac.apple.com (130.43.2.3)
Location: /pub/stud_reps

faui43.informatik.uni-erlangen.de (131.188.31.3)
Location: /portal/mounts/cyber/pcd/freeware2/magazine

srawgw.sra.co.jp (133.137.4.3)
Location: /.a/sranha-bp/arch/arch/comp.archives/hackers/sites

---

What's Your NPA These Days?

<><><><><><><><><><><><><><><><><><><><>
<> <>
<> AREA CODE SPLITS OF 1991 <>
<> Researched and Collected <>
<> by <Flash!Point> <>
<> <>
<><><><><><><><><><><><><><><><><><><><>

BALTIMORE, MARYLAND
C&P Telephone Company Report for 301 NPA Split

NXXs Converting to NPA 410

205 208 213 221 222 224 225 226 228 232 233 234 235 237 239 242 243 244 247 250
252 254 255 256 257 260 263 265 266 267 268 269 272 273 275 276 278 280 281 282
284 285 287 288 289 290 291 296 298 307 312 313 316 319 321 323 325 326 327 328
329 332 333 335 337 338 339 342 343 346 347 348 351 352 354 355 356 357 358 360
361 362 363 364 366 367 368 370 374 376 377 378 379 381 382 383 385 388 389 391
392 393 396 397 398 404 425 426 429 433 435 437 438 440 442 444 446 448 450 452
455 456 457 458 461 462 465 466 467 471 472 476 477 479 481 482 483 484 485 486
488 489 494 514 515 516 521 522 523 524 525 526 527 528 529 531 532 533 534 535
536 537 538 539 541 542 543 544 546 547 548 549 550 551 553 554 555 556 557 558
560 561 562 563 566 569 573 574 575 576 578 581 583 584 586 591 592 594 597 602
605 612 613 614 623 624 625 626 628 631 632 633 634 635 636 637 638 639 641 642
643 644 646 647 648 651 653 655 658 659 661 664 665 666 667 668 669 671 672 673
674 675 676 677 679 682 683 684 685 686 687 691 692 693 712 715 719 720 721 723
726 727 728 730 732 734 740 741 742 744 745 747 748 749 750 751 752 754 755 756
757 758 760 761 764 765 766 768 771 775 778 780 781 783 784 785 787 788 789 792
793 795 796 798 799 806 813 819 820 821 823 825 827 828 830 832 833 835 836 837
838 841 844 848 849 850 857 859 860 861 866 867 873 875 876 877 879 880 882 883
885 886 887 889 892 893 896 906 915 920 922 923 928 931 936 938 939 941 943 944
945 947 950 954 955 956 957 960 962 964 965 966 968 969 971 974 976 978 979 987
988 991 992 993 995 996 997 998 999

- -

SAN FRANCISCO, CALIFORNIA
Pacific Bell Customer Report For 415 NPA Split

NXXs Converting to NPA 510

204 208 210 215 222 223 226 228 229 231 233 234 235 236 237 238 245 248 251 253
254 256 261 262 263 264 265 268 269 271 272 273 275 276 277 278 279 283 284 287
293 294 295 297 298 302 307 309 310 313 317 339 351 352 356 357 370 372 373 374
376 385 410 412 414 416 417 419 420 422 423 425 426 427 428 429 430 432 436 437
438 439 440 443 444 446 447 448 449 451 452 455 458 460 462 463 464 465 466 471
475 481 482 483 484 486 487 489 490 498 504 509

==Phrack Inc.==

Volume Four, Issue Thirty-Eight, File 3 of 15

==Phrack Pro-Phile==

Written by Dispater

Created by Taran King (1986)

Welcome to Phrack Pro-Phile. Phrack Pro-Phile is created to bring info to you, the users, about old or highly important/controversial people. This month, I bring to you the original of the controversial New TAP Magazine.

Aristotle

Personal

Handle:	Aristotle
Call him:	Kevin
Past handles:	Ed, Bob, Bill, and a multitude of other lame handles.
Handle origin:	Humanities class in high school.
Date of Birth:	April 12, 1970
Age at current date:	22
Height:	5'10"
Weight:	145 lbs.
Eye color:	Blue
Hair Color:	Red
Computer:	IBM-PS/2 55SX
Sysop/Co-Sysop of:	ALL PAST: Digital Underground, Blitzkreig, some board on a major packet switching network, a board on MIT's FSF machines, and a bazillion other lame boards that I don't care to mention.

I was one of those people that played with phones for as long as I can remember. I guess you could say I started phreaking a few years before WARGAMES came out. After the movie, I found out that other people were interested in phones too. Due to the influx of "elite hackers" after the movie, information became extrememly available. This lead to my existence in the real world of hack/phreak.

Eventually I ended up writing articles for both 2600 and TAP. In the late 80s I restarted TAP with help from some friends and we started to revive one of the first hack/phreak magzines that ever existed.

Having TAP helped us gain a special insight on how the system really works. Some of our issues were cool enough to actually be censored at certain institutions where avid censorship still exists. Also, we were allowed to see how far you could go in expressing your opinion until some bigshot noticed.

Believe it or not though, running a periodical without any income is a major pain. It was well worth it though as I got to meet a lot of cool people and also was able to do something for the computer underground scene. If you currently don't support magazines like 2600, etc., please do. They are doing a lot of work for the community and without them, there would be a major gap in the press regarding the truth about our community.

I exited the hack/phreak world when things got a bit hairy and Craig (Knight Lightning) got nailed. I simply decided that a hobby is not worth going to jail for and that it did not pay the bills either. Anyways, most old hacks eventually reach the point where everything they see seems old and boring. This is where I currently am.

Today I am employed at a computer lab at a large university where I am working on a degree.

Aristotle's Favorite Things
~~~~~~~~~~~~~~~~~~~~~~~~~~~

```
      Women:  Karen (To be married soon)
       Cars:  REAL Cars:  '86 Mustang GT, '86 VW Golf, various Porsches.
      Foods:  Anything that you cannot get at a drive-thru.
      Music:  Metallica, Bach, Danzig, Anthrax.
    Authors:  All the posters of Alt.Sex
      Books:  The Art of War
Outdoor fun:  Snowboarding
```

Most Memorable Experiences
~~~~~~~~~~~~~~~~~~~~~~~~~~

- Getting engaged
- My first blue box call
- Watching some guy die after wrecking his car
- Being interviewed by the FBI for something I did not do and then pissing them off by allowing them to prove that they were wrong.
- All of the SummerCons and other assorted h/p meetings.

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

- Bill from RNOC : Getting us kicked out of the museum at the Arch.
- Cheshire Catalyst : Help with restarting TAP.
- Slave Driver : For his hospitality and the infamous "Guess who/what died in the couch" game.
- The Mentor : For the BBS and his non-snobbish attitude.
- J.R. "Bob" Dobbs : All the cool blue box info.
- The Not : All the help with Unix
- Taran King : For being an exception to the "Hackers are all geeks" rule.
- Knight Lightning : For sending back the pictures and generally being a cool guy.
- Dispater : For having the no-bullshit attitude and actually getting the job done.
- Nite Ranger : For helping me realize that lamers will always exist (not you though).
- Predat0r : All the experiences.
- All the Legion of d0oDs : For adding to the entertainment at PartyCon.

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

Of the general population, I would consider about 89.9% to be nerds. I would also consider 65% of the entire population nerds and/or strange. Phreaks may be geeks but each usually has his/her cool qualities as everyone does. Most are socially lacking though. Keep in mind that a hacker/phreak is ALWAYS better than the average GIF viewing geek.

~~~~~~~~~~~~~~~~~~~~~~

==Phrack Inc.==

Volume Four, Issue Thirty-Eight, File 4 of 15

Pirates' Cove
Issue Two

By Rambone

Welcome to Issue Two of Pirate's Cove. There is a lot going on in the Pirate community, busts of pirates in the USA and Canada, and new software and operating systems like IBM's OS/2. So sit back and absorb the news.

First on the agenda is to discuss the over-talked about, and hopefully dead issue of the carding scam initiated by The Grim Reaper and The Not So Humble Babe. The reason Phrack Magazine delayed publishing anything about this bust was because we refused to publish any third party rumors and idle gossip. Now that I have personally spoken with the Grim Reaper, we can shed some light on this subject.

Mike "The Grim Reaper" obviously regrets what has transpired and would like to put this part of his life behind him. At this point in time, he still does not know what is going to happen, and is taking his arrest very seriously. Mike asked me just to use the letter he has written. Some of you may have seen this before, some may not.

****

Statement by The Grim Reaper

"Lamer Pirate Magazines, Etc..."
By THE GRIM REAPER

This was originally going to be an article for iNSANITY Magazine #4 called "Lamer Pirate Mags, Etc." to straighten out the complete bullshit and lies in Badnews #7, but seeing as there are so many rumors floating around, and the future of iNSANITY is undecided, I decided to just put out this text file to explain what is really going on, less a few lamers out there spread all kinds of bullshit and lies, as they seem to do so often.

Pretty much everything in Badnews #7 was a complete lie, as most of you already know by now. They didn't have any backdoors to ViSiON-X, and there aren't and weren't any that allowed someone to get the user list. What happened on Showdown was the Sysop PW was given out to the wrong person, and they used it, so again, nothing but B.S. and hype on their end. While I think the FiRM overhyped themselves, they didn't deserve the ragging they got by BaD, and BaD having failed in their own attempt at a pirate group has no right to criticize ANYONE until they've accomplished the same. Perhaps a few of the other groups could have said something to them (and many talked about it) but they didn't deserve the 3rd Degree from a lamer mag.

The main reason for this article was that while many found the BaD Mag to be so completely full of shit to the point that it was hilarious, some got to thinking that down the line, someone might actually believe some of the B.S. They claimed to be the group that caused the downfall of THG, PE and others, which was a complete joke... They had absolutely nothing to do with any of that. USA had killed off THG, etc... What else was there to straighten up?

"Did they shoot your Dog????"
- Anonymous Lamer

So what's up? Well, to make it short and blunt, The NotSoHumble Babe and I were involved in a carding incident. She most likely was being watched by certain people since she had been using false corporations and fake Tax ID Numbers to order games and for suppliers for USA. The Secret Service either stumbled across us that way, from one of the orders gone bad, or from the illegal cash and hardware coming in to Enterprize. The NSH Babe (Amy) had a cash flow from Dist Sites and other hot hardware from USA Sites totalling about

$3500-$5000 a month. She had sent one of her hot laptops she gets every month to Optical Illusion in Canada, and asked him to sell it for her. He wanted to be nice and tried to sell it. A local from his 416 area wanted to buy the laptop. He went to sell it, and was busted by a plainclothes police officer for possession of stolen property of over a $1000.

I found some CC #'s, she had a lot of experience with UPS and FedEx from ordering games, and she thought of a way to pick up the packages. We both placed orders (I placed about 2/3rds since she was picking up, and she placed about a 1/3rd). Most of the stuff wasn't for myself, and was meant for other people (trying to be nice, eh?). In any case, we shouldn't have done it. TNSH Babe wanted to order a A LOT of stuff because, over time, she owed people in USA a lot of hardware they had paid her for, and she had never sent any to them. We ordered a bit too much, more than I thought we should have.

"They had Bulletproof Vests and Grenades??"
- Another |<-Rad D00D!!

So then what? Well, they found out the packages were coming and were waiting for TNSH Babe to pick them up. They went back to her place and she gave them permission to come in and search (dunno what happened in between then). She talked to them and they wanted to have her give some of the stuff to me that she got when we were supposed to meet for the first time at a Meijers parking lot. There were some weird things going on at the time, and an alarm was flashing in the back of my mind, but I decided to ignore it. Anyhow, she handed me a hard drive or something, then, basically, they moved in. I saw a car pulling up, and figured what was going on. One guy said, "Secret Service" (about 6 people), and it kinda went downhill from there. But seriously, they weren't that bad and I cooperated with them.

They wanted to go back to my house and look around, and wanted permission. They said they would have gotten a search warrant, and it was in my best interest to cooperate, so I let them come in. Basically there wasn't anything in the house, I always throw everything out when I am done with it. As far as the computer went, I didn't even have anything Unzipped on the Hard Drive that I hadn't paid for. They wanted to look further on the computer and in the end did take it, but gave me a receipt. I paid for my entire system, so don't listen to some of the lamer textfiles floating around. There wasn't anything on my system, so I might get lucky and they'll give it back. They also took 3 or 4 computers from Amy's place, but left Static with his. This was the first time either of us had done anything like this. There had been a few attempts in the past, but nothing that had ever been followed through, or had worked. No no, I've never been busted for this before, or anything. I've never been arrested for anything before.

"I formatted my Hard Drive 3 Times!!"
- Local 313 Sysop

I don't know if it was overreacting, but our dumb situation seemed to affect a lot of other people. The locals over here went apeshit, and many of them formatted their drives and deleted files (20+), and took their boards down temporarily. Many of the major pirate boards decided to power down for a while. Unfortunately many of the truly good boards in the world have gone down, possibly forever. BBS-A-Holic has gone down, Enterprize is now PD Only, many INC boards, LSD2 possibly for related reasons, The VOID of course, and many others. Many big names are considering quitting the pirate scene because they think it's not worth it, and they're right. Some of the boards may come back. BBS-A-Holic was one of my favorites. Many considered The VOID one of the Top 10 Boards in the world as far as quality went, and I appreciate the users and the support. I worked hard to try to make it the best, and put my heart into it. As are many others, Black Spyrit might be retiring, so I don't know if another iNSANITY Issue will be coming out. It was truly a great mag if you never saw it. The best.

"I heard they were thrown in jail, and fined $72 Million Dollars!!"
- Another Neverending Lamer

No matter what or who the issue, this never stops, eh? I wouldn't believe

any of the bullshit text files, mostly from jealous people and the few enemies you get when you end up getting towards the top, especially the anonymous (surprise) text file taken off of OOFNet (surprise again, huh? Heh). All are, as always, complete B.S.

Try not to be a lamer. There are too many of 'em, and they do nothing for the pirate world. If you are going to do anything, do SOMETHING. Organize a group of some type, coordinate couriers, do some VGA or ANSI work, or get in a group, but don't be a lamer. Call LD, establish a rep, and see what you are missing. All locals aren't lamers, but 90% are.

A Lamer - A person who calls only local boards, does nothing but leeches files, and doesn't contribute to groups in any ways.

Neither BaD, any locals, or Socrates had anything to do with us getting into trouble in any way.

"Don't try this at home kids."
- Grim '92

All things considered, I wish it wouldn't have ended this way. I don't think any of this was good for anyone in the pirate or BBS world. USA is now pretty much a dead group. Many of the best boards have gone down, and others are considering calling it quits because it just isn't worth it. INC never was a for-profit group, and had no illegitimate cash flow, unlike USA.

****

Rambone's Remarks
~~~~~~~~~~~~~~~~~

Well that's the real story, straight from the horse's mouth. I've read at least a dozen text file's after this one, and I tend to believe what Mike has written. Now Amy (NotSoHumble Babe) tells a different story. According to her text file, she had seldom carded or phreaked before, but no one seems to be able to corroborate this information, and people that know her tend to say she was in deeper than she cares to admit. It's also been brought to my attention that Amy may be volunteering information to the feds about other people. What she has done before or after the bust may or may not be true, but here is her story.

****

Statement by The Not So Humble Babe
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Well, I am sure you have all heard that I had a small legal problem today, and I know how stuff gets blown out of proportion, so I thought I'd explain the story myself. Here goes...

I have carded a few items in the past 3 days, and I have NEVER done this before. The Grim Reaper got CBI accounts and placed orders, and I picked them up. Well, one of the places Grim ordered from was Paradise Computers. They knew it was a bogus order, but told us the package was shipped. Then they called the FEDS. Anyhow, the Feds must have been watching the pickup spot, then following me around until I met up with Grim to deliver his share of the stuff. As soon as we went to make the exchange, the Secret Service, FBI, state police, and local police were running at us with bulletproof vests and automatic guns. They handcuffed us, separated us, and took each of us back to our homes for them to search.

I haven't talked to Grim Reaper since I saw him lying next to me on the ground being arrested. But here's my story. About 20 agents came to my apartment and grabbed all computer equipment without a receipt. So we still have 1 modem, and this computer system. Anyhow, they grabbed every piece of paper they could find. Unfortunately, I am a very organized person, and had "the who's who in the pirate world" written down for my use. So if you ever gave me your real name, number, or address, it is now in the hands of the Secret Service and FBI. This list was quite large, as it took 2 years to compile.

These boys did their homework. They knew Enterprize was USA HQ and they

knew my handle, and they knew I supplied the group with software. They weren't going for just anyone here guys; they knew they needed to bust a group leader. Well, they did. Got me on carding, pirating, and a ton of other legal terms having to do with both of these.

I was charged with 6 different counts, each holding a 5-30 year prison sentence. It doesn't look good for me at all. I'll post a file as soon as I get arraigned and let you guys know what is going on.

But I will say this now, and I MEAN it. I love the groups, the software, and the competition. But regardless of what happens to me, I am done forever. No more NotSoHumble Babe, no more USA. I hate to do this to everyone, but I really don't have a choice. And regardless of who I am that got busted, be strong and support what you believe in your hearts: PIRACY. Don't let them win. You guys can all go on without me. Just promise me you won't give up and throw in the towel. If anyone wants to contact me, you can leave e-mail on Enterprize for me, or call voice AT YOUR OWN RISK. They told me they were tapping the phone lines.

****

News Flash: Mutli-Media Aggravation

Mutli-Media games (CD-Rom) are being played on the hard drive. There seems to be a trend of starting to send out huge CD-Rom games electronically through BBSes, the first one being Battle Chess I, and taking as much as 30 megs of hard-drive space. Soon after, Steller 7, and Wing Commander I started to show up. One of the reason for the start of this was a lack of programs coming down the pike, and one group decided to send Battle Chess out. I haven't seen anything lately, and hope programs meant for the CD-Rom will stay that way.

****

Another News Flash: OS/2 2.0 GA

IBM has released the long anticipated OS/2 (Operating System 2) 2.0 GA. OS/2 2.0 is an alternative to DOS 3.3, 4.01, or the latest, 5.0, and implements true 32 bit technology. There are several ways of using this operating system. OS/2, implementing it's own version of FAT, Dual Boot (which will allow you to be able to use DOS if necessary), and a Multi-Boot, brings up a prompt a when booting up which allows you to choose which operating system you would like to use (similar to Vpix for Unix and Xenix).

I had the opportunity to view a preview of OS/2 2.0 GA at our local IBM Corporate Building, and to say the least, I was impressed. One of the points stressed at the meeting was the diverse control over many programs at the same time. OS/2 comes with its own operating system, along with a clone of sorts of both DOS and Windows. This feature will enable a user to access a DOS emulation without having to actually boot up DOS on the machine. It also has a Windows emulation which will eradicate the need for a full blown version. The one shortcoming of this is that it is Version 3.0, but I have been informed that 3.1 is right around the corner, and actually saw a demonstration of it.

The true strong point of OS/2 is the mutli-tasking. After witnessing 15 windows open at the same time, all with programs running concurrently, I truly can say this is a step into the future, and it is here now. My personal experience running 2.0 is very impressive. Being able to properly run a program with the BBS in the background is a welcome treat, and I see no reason to ever support another operating system, until I get my hands on Windows NT.

****

Industry News

The long awaited A-10 Avenger by Spectrum Holybyte has now been pushed back till early next year. This was the next in a series of interactive programs put out by SH to be played over the modem, the first being Falcon 3.0, a 256VGA jet game.

UT (Ultra-Tech) and EMC (Electro-Magnetic Crackers) have now merged. This merger will be beneficial to both groups, bringing lacking talents together to form one of the largest cracking groups in the world, one with strong software connections, and the other with cracking resources and existing software support sites. Captain Tom of UT and Cyborg of EMC brought the whole thing together as a reality, and this merger may point them in the same direction as when INC formed their group from several smaller groups.

****

BBS Bust in Canada
~~~~~~~~~~~~~~~~~~

The Federal Investigations Section of the RCMP seized components of an electronic bulletin board system (BBS) "90 North" at a West Island residence. This is believed to be the first execution of a search warrant under the Copyright Act of Canada against an electronic bulletin board system.

The seizure included 10 micro computers, seven modems and the software present on these systems (approximate value of $25,000). An electronic bulletin board is a service which allows personal computer users to exchange messages and to exchange or receive computer files including software, text and digitized images over telephone lines via a modem.

During a four-month investigation, it was established that the 90 North BBS enabled users to obtain software in exchange for other files or for an annual fee of $49.00. While some of the programs consisted of "shareware" which may legally be distributed in this way, much of the available material was protected under the Copyright Act including beta versions of commercial software packages which have not yet been released on the market. More than 3,000 software programs were available to users of this BBS including WordPerfect 5.0, Microsoft DOS 5.0, Windows 3.0, Lotus 1-2-3 for Windows, Borland C++ 2.0, Quattro Pro 3.0, d-Base IV 1.1, SCO Xenix for DOS, Netware 3.11 and Clipper 5.0.

Charges of commercial distribution of pirated software are planned against the owner and operator of 90 North. Paragraph 42 (1)(c) of the Copyright Act states that "every person who knowingly distributes, infringes, copies of any work in which copyright subsists either for the purpose of trade or to such intent as to affect prejudicially the owner of the copyright, is guilty of an offense and liable on summary conviction, to a fine not exceeding $25,000 or to imprisonment for a term not exceeding six months or to both, or on conviction on indictment, or a fine not exceeding $1 million or to imprisonment for a term not exceeding five years or both."

More Details On The Canadian BBS Bust
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

The Royal Canadian Mounted Police (RCMP) has, for the first time under the Copyright Act of Canada, seized all the components of an electronic bulletin board (BBS), for providing illegal copies of copyrighted software to its subscribers.

According to Allen Reynolds of the secretariat of the Canadian Alliance Against Software Theft (CAAST), the Federal Investigations Section of the RCMP has not laid formal charges against the West Island, Quebec owner and operator of the BBS. Charges of commercial distribution of pirated software are planned against the owner of 90 NORTH, he said.

CAAST is a Canadian organization made up of ASHTON-TATE CANADA, LOTUS DEVELOMENT CANADA, MICROSOFT CANADA, NOVELL CANADA, and QUARTERDECK OFFICE SYSTEMS CANADA. Its main objective is to educate the public and business about the hazards of software piracy.

In the raid, the RCMP seized 10 Micro computers, seven modems, and about $25,000 worth of software which was allegedly being distributed to users of the 90 NORTH BBS for an annual $49.00 fee, Reynolds said.

Some of the seized software packages were Wordperfect 5.0, MS-DOS 5.0, Windows 3.0, Lotus 1-2-3 for Windows, dBase IV, Netware 3.11, and Qemm. If charged and convicted on a summary conviction, the 90 NORTH owner could face

either a penalty or a fine not exceeding $25,000 or a jail term not exceeding six months or both. If the 90 NORTH owner is convicted on indictment, the penalty is a fine not exceeding $1 million or imprisonment for a term not exceeding five years or both. "I don't know how long it will take to lay charges," Reynolds said. He would not speculate when the RCMP would charge the owner of 90 NORTH, but he did say that the users of the 90 NORTH BBS will not be investigated by by the RCMP.

He added that there is reason to believe that a number of BBSes across Canada are supplying beta test versions of products which can be dangerous to a user's system because they are usually laced with bugs.

****

Rambone's Remarks
~~~~~~~~~~~~~~~~~

I have been informed that there are several more bulletin boards, especially those in the 416 NPA, that are under investigation right now. Most of the sysops being busted are ones that charge for download credits, which is a violation of the Copyright Act for reselling software.

****

New Release
~~~~~~~~~~~

Ultima UnderWorld by Origin
Name: The Stygian Abyss
Company: Origin
Graphics: 256VGA
Sound: SB/SB-Pro/Adlib/Roland
Rating: 10/10
Supplier: High Pockets/Red Runner
Copy Protection: None
Date: 3/26/92

Looking for virtual reality in a game? Didn't think you could find it? Welcome to Origin's Ultima UnderWorld, "The Stygian Abyss." Don't let the name fool you, this game does not have any attributes from the Ultima 1-6 series. You start out in a dark room looking out into what would be called a 3-D perspective. Picking up the bag in front of you would be your best bet -- it may have things that you need. Once you are on your way, you will notice how realistic the walls, ground, and ceiling look, almost like you are there. Along the way in your adventure, you will encounter many items that will help you along the way and some that may not, but you will have to decide. There are also many cultures down below that will be friendly and not-so-friendly; use your best judgement. Learn all your abilities. They will come in handy down the road. Practice your magic, it may save your life, or help you walk across water (hint). Learning how to jump correctly is important. You'll have to be able to leap across flaming, volcanic ravines to be able to finish the game. When you see writing on the wall or in a scroll with words and telling you to chant this to the Mantra, you better copy them down: They build up your attributes.

All in all, there are 7 levels, and one unexplored level, sporting true 256VGA graphics, SB-Pro support, and a riveting sound-track. This is this closest thing to virtual reality graphics in the game market today, and it'll be a while before you play anything else like it.

==Phrack Inc.==

Volume Four, Issue Thirty-Eight, File 5 of 15

Network Miscellany IV
Compiled from Internet Sources
by Datastream Cowboy

Network Miscellany created by Taran King

Special Internet Connections February 5, 1992
~~~~~~~~~~~~~~~~~~~~~~~~~~~ Most Recent Update

Comments to: Scott Yanoff <yanoff@CSD4.CSD.UWM.EDU>

American Philosophy Association
telnet atl.calstate.edu or 130.150.102.33
Login: apa
OFFERS: BBS for APA.

Archie
telnet archie.mcgill.ca or 132.206.2.3 (Canada)
telnet archie.funet.fi or 128.214.6.100 (Finland/Europe)
telnet archie.au or 128.184.1.4 (Australia/New Zealand)
telnet cs.huji.ac.il or 132.65.6.5 (Israel)
telnet archie.doc.ic.ac.uk or 146.169.3.7 (United Kingdom/Ireland)
telnet archie.sura.net or 128.167.254.179 (Maryland, USA)
telnet archie.unl.edu (Password: archie1) (Nebraska, USA)
telnet archie.ans.net or 147.225.1.2 (New York, USA)
telnet archie.rutgers.edu or 128.6.18.15 (New Jersey, USA)
OFFERS: Internet anonymous FTP database. (Login: archie)

Archie Mail Servers
mail archie@<INSERT ONE OF ABOVE ADDRESSES HERE>
Subject: help
OFFERS: Alterative Archie access to those without ftp or telnet access.

Automated Data Service
telnet tycho.usno.navy.mil or 192.5.41.239
Login: ads
OFFERS: Navigational/Time/Astronomical Information.

CARL
telnet pac.carl.org or 192.54.81.128
OFFERS: Online database, book reviews, magazine fax delivery service.

CHAT
telnet debra.doc.ca or telnet 192.16.212.15
Login: chat
OFFERS: Conversion of Hypertext Access Technical information files.

Cheeseplant's House
telnet orchid.csv.warwick.ac.uk 2001 or 137.205.192.5
OFFERS: Online chat service in a very unique format.

Chess Server
telnet lark.utah.edu 5000 or telnet 128.110.128.72 5000
OFFERS: Play/watch real-time chess with human opponents.
Type "help" for help

C64 Archive Server
mail twtick@corral.uwyo.edu
Subject: Mail-Archive-Request Body-of-letter: help (hit return) end

Dante Project
telnet library.dartmouth.edu or 129.170.16.11
Login: connect dante
OFFERS: Divine Comedy and reviews.

Distance Educational Data
~~~~~~~~~~~~~~~~~~~~~~~~~~~

```
     telnet sun.nsf.ac.uk or telnet 128.86.8.7
     (Login: janet  Hostname: uk.ac.open.acs.vax  Username: icdl)

Document Site
     ftp ocf.berkeley.edu or ftp 128.32.184.254
     OFFERS: Many docs, including 5 purity tests, the Bible, lyrics.

Earthquake Information
     finger quake@geophys.washington.edu
     OFFERS: Recent quake information (location, time, magnitude, etc.)

E-Math
     telnet 130.44.1.100 (Login: e-math  Password: e-math)
     OFFERS: American Math Society sponsored BBS with software and reviews.

FEDIX
     telnet fedix.fie.com or telnet 192.111.228.1
     Login: fedix
     OFFERS: Information on scholarships, minority assistance, etc.

Freenet
     telnet freenet-in-a.cwru.edu or 129.22.8.82 (Cleveland)
     telnet yfn.ysu.edu or 192.55.234.27 (Youngstown)
     OFFERS: USA Today Headline News, Sports, etc.

FTP Mail
     mail ftpmail@decwrl.dec.com
     Subject:(hit return) Body-of-letter: help (return) quit
     OFFERS: ftp via e-mail

Genetics Bank
     mail gene-server@bchs.uh.edu
     Subject: help
     OFFERS: Genetic database accessible via e-mail.

Geographic Server
     telnet martini.eecs.umich.edu 3000 or 141.212.100.9 3000

Gopher
     telnet consultant.micro.umn.edu
     Login: gopher
     OFFERS: Access to many interesting features.

Graf-Bib
     mail graf-bib@decwrl.dec.com
     Subject: help
     Body-of-letter:  send index
     OFFERS: Graphics bibliography

Ham Radio Callbook
     telnet marvin.cs.buffalo.edu 2000 or 128.205.32.4 2000
     OFFERS: National ham radio call-sign callbook.

INFO - Rutgers CWIS
     telnet hangout.rutgers.edu 98 or 128.6.26.25 98
     OFFERS: Dictionary, thesaurus, CIA world fact book, quotations database.

Internet Resource Guide
      ftp nnsc.nsf.net
      OFFERS: Compressed/tar'd list of net resources in /resource-
              guide.txt.tar.Z

IRC Telnet Client
     telnet bradenville.andrew.cmu.edu or 128.2.54.2
     OFFERS: Internet Relay Chat access.

Library of Congress
     telnet dra.com or 192.65.218.43
     OFFERS: COPY of Library of Congress
     (Assumes terminal is emulating a vt100)
```

```
List of Lists
      ftp ftp.nisc.sri.com or ftp 192.33.33.22
      mail mlol-request@wariat.nshore.ncoast.org
      OFFERS: List of interest groups/e-mail lists in /netinfo/interest-groups.

Lyric Server
     ftp cs.uwp.edu
     OFFERS: Lyrics (/pub/music/lyrics/files) in text files for anonymous ftp.

Mail Server/User Lookup
     mail mail-server@pit-manager.mit.edu
     Usage: In body of mail message: send usenet-addresses/[name searching for]

Melvyl
     telnet melvyl.ucop.edu or 31.1.0.1
     OFFERS: Access to various libraries.
     Type "other" at prompt to see others.

NASA Headline News
     Finger nasanews@space.mit.edu
     OFFERS: Daily press releases from NASA.

NASA SpaceLink
     telnet spacelink.msfc.nasa.gov or 128.158.13.250
     OFFERS: Latest NASA news, including shuttle launches and satellite
             updates.

NED
     telnet ipac.caltech.edu or telnet 131.215.139.35
     Login: ned
     OFFERS: NASA Extragalactic Database.

NetLib
     mail netlib@ornl.gov
     Subject:(hit return)
     Body-of-letter: send index
     OFFERS: Math software.

Oceanic Information Center
     telnet delocn.udel.edu or telnet 128.175.24.1
     Login: info

Oracle
     mail oracle@iuvax.cs.indiana.edu
     OFFERS: The Usenet Oracle!
     Mail with subject as "help" for more info.

PENpages
     telnet psupen.psu.edu or telnet 128.118.36.5
     Login: PNOTPA
     OFFERS: Agricultural info (livestock reports, etc.)

SDDAS
     telnet espsun.space.swri.edu 540 or telnet 129.162.150.99
     OFFERS: SW Research Data Display & Analysis Center.

SERVICES
     telnet wugate.wustl.edu or 128.252.120.1
     Login: services
     OFFERS: Access to nearly every listed service!

Software Server
     telnet charlie.secs.csun.edu 5742 or 130.166.2.150 5742
     OFFERS: Similar to Archie.
     Type help for a list of commands.

StatLib Server
     mail statlib@lib.stat.cmu.edu
     Mail with line: send index.
```

```
     OFFERS: Programs, Datasets, etc. for statisticians.

STIS
     telnet stis.nsf.gov or 128.150.195.40
     Login: public
     OFFERS: Science & Technology Information System.

Supreme Court Rulings
     ftp ftp.cwru.edu
     OFFERS: ASCII files of Supreme Court rulings in directory /hermes

Usenet News MailServer
     mail [newsgroup]@ucbvax.berkeley.edu
     Allows you to post to a Usenet newsgroup via e-mail.  Useful if you have
     read-only access to Usenet news.
     Note: .'s become -'s  Ex. alt.test -> alt-test

UNC BBS
     telnet samba.acs.unc.edu or 128.109.157.30
     Login: bbs
     OFFERS: Access to Library of Congress and nationwide libraries.

WAIStation
     telnet quake.think.com or 192.31.181.1
     Login: wais
     OFFERS: Wide Area Information Service
     FTP think.com for more info.

Weather Service
     telnet madlab.sprl.umich.edu 3000 or 141.212.196.79 3000
     OFFERS: City/State forecasts, ski conditions, earthquake reports, etc.

World-Wide Web
     telnet info.cern.ch or telnet 128.141.201.74
     OFFERS: Information service with access to various documents, lists, and
     services.

  * NOTE: NO LOGIN NAMES OR PASSWORDS ARE REQUIRED UNLESS STATED OTHERWISE! *
    If it prompts you for a login name, you did something wrong, or are not
        running on a machine that the system you telnetted to supports!
```

```
   +++++ Zamfield's Wonderfully Incomplete, Complete Internet BBS List +++++

FOREWORD
~~~~~~~~
The following list has been compiled with the help of the wonderfully generous
crowd of folks who associate with Internet or UseNet.  I owe them many thanks
and please keep the info coming.

I, and many others, have a few things to say about these BBSes in general.  So
bear with me, or skip ahead, but do take a look later.

1). These BBSes are provided as a service to anyone on Internet.  Not just you.
2). While you may not directly pay for these services someone does.
3). You are a guest, and please keep that in mind while using these BBSes.

Okay, that wasn't so bad after all.

Most of these BBSes offer services unique to BBSing.  Some offer small scale
versions of standard Internet services.  Keep in mind that mail or articles
posted on BBSes do not reach everyone in the world, and if you can get to
UseNet, you will probably find better responses.  Most of the files on these
BBSes can be found by anonymous FTP, so don't tie up the system with files if
you have FTP.  Do be considerate on these BBSes, some people aren't using
telnet or rlogin to get to these, some people still dial numbers with modems at
their homes. :-)

For users of JANET (UK), you may access these BBSes through first connecting to
UK.AC.NFSNET-RELAY.TELNET or PAD.UK.AC.NFSNET-RELAY.TELNET.  Likewise, users of
```

Internet can get to JANET by telnet SUN.NFS.AC.UK, login as janet.

Zamfield@Dune.EE.MsState.Edu

==========

2/6/92

NAME ADDRESS LOGIN BBS Software

AfterFive winner.itd.com 9999
-- 128.160.2.248 9999

-- Hours: 5 p.m. to 8 a.m. CST. Please no logins during the day.

-- MUCK - enhanced tinymuck2.2.3d-beta. Based on Bourbon Street, New Orleans. May not be appropriate for all ages, especially very young children as the database is rather graphic in section describing strip tease, and bars.

-- BBS is Citadel like Quartz and Grind. No HotKeys though. Supports 59 concurrent users.

-- This site is running on a very fast machine, but you might experience network delays. Contact Howard, Darrel, Trish, Wolvercuss, Akbaar or Captain, wizards, if you wish to work on any aspect of After-Five.

BadBoy's Inn 130.18.80.26 bbs Pirate 2.0
-- badboy.itd.msstate.edu

-- Boards, Talk, Chat, Mail
-- Test site for new Pirate Software.
-- Pirate 2.0 kicks, if it would work all the time!

Campus_d 35.204.192.2 LOGIN CAMPUS_D
-- umde.dbrn.umich.edu

-- Currently down and contemplating permanent removal. (8/2/91)
-- Send comments/condemnations/pleading/apologizing/reminiscing/etc. to DEN@UMDE.DBRN.UMICH.EDU

Cimarron (in Spanish) bugs.mty.itesm.mx bbs Pirate 1.0
-- 131.178.17.60

-- Nice BBS, too bad it is all in Spanish. Good place to get acquainted with if you are trying to learn Spanish, lots of conversations to look at. Cimarron means Wild Dog or Untamed.

-- This BBS seems to be a limited access site. I have gained access only during late hours CST. I will try to get more info on this.

Cleveland Free-Net 129.22.8.75 (cwns16.ins.cwru.edu) CWRUBBS
-- 129.22.8.76 (cwns9.ins.cwru.edu)
-- 129.22.8.82 (cwns10.ins.cwru.edu)
-- freenet-in-a.cwru.edu
-- freenet-in-b-cwru.edu
-- freenet-in-c-cwru.edu

-- Usenet, Internet, MUD, USA Today Online. Local mail, and Interest Groups.

CueCosy cue.bc.ca cosy Cosy 4.0
-- 134.87.11.200

-- Conferences and Topics, EAN Mail, Usenet, FTP, downloads Kermit & Xmodem, Online Unix course, some local files.

Cybernet Waffle BBS 131.91.80.13 bbs Waffle
-- shark.cs.fau.edu

-- Nice BBS, but I still haven't gotten word on whether I have been validated

or not. And no response to my mail either. Lots of conferences, and Magpie Chat. Information for Floridians, GNU, computers, alternate PUBNET, recreational, science, social, Unix-PC; unsure about files, but still nice.

Delft University BBS 130.161.180.68 BBS
-- tudrwa.tudelft.nl

-- In Holland, mostly Dutch.
-- Files, messages, chat areas

Endless Forest 137.48.1.5 2001
-- forest.unomaha.edu 2001

-- Boards, E-mail. Reminds me of WWIV BBS.

Hall of Doom servax.fiu.edu
-- 131.94.64.2

-- login as WEATHER, passwd WEATHER
-- select 666
-- login as new.

Heartland Peoria Illinois FreeNet
-- 136.176.10.10 fnguest
-- heartland.bradley.edu

-- Mail, Public Forum, Recreation, Calendar, Social services, Senior center, Teen center, Local job & government information, Legal, Medical, Tax, & Invest/Banking Forums SIGs, Library, Home & Garden, Science & Tech, & Education Forums.

Hewlett-Packard BBS hpcvbbs.cv.hp.com
-- 15.255.72.16

-- has tech help, and 48SX files/programs.

IDS DataForum 192.67.241.11 guest
-- ids.jvnc.net

-- IDS DataForum is a public access system run on a DEC VAX. It is menu driven, supports VT100, and ANSI graphics.

-- Features, TELNET, FINGER, Weather Underground, Ham Callsign Book. Adds Internet Mail (VMS Mail).

-- Includes Entertainment, such as, International MUDs, local-only games, CONQUEST & GALACTIC TRADER, and CB Simulator for CHATS.

-- RIME, PC-BBS messaging network, Usenet NEWS with "nearly" full newsfeed.

-- DialOut service, online Game Developer Conference, and BBS software available as well.

-- Local access at (401)-884-9002, (V.32, Telebit/PEP, USR HST, V.42bis).

-- More info at ids-info@idsvax.ids.com

ISCA isca01.isca.uiowa.edu iscabbs DOC (Citadel)
-- grind.isca.uiowa.edu
-- 128.255.19.233
-- 128.255.19.175

Mars Hotel Mars.EE.MsState.Edu bbs Pirate
-- 130.18.64.3

-- Boards, Talk, Chat, IRC, Mail.
-- Fairly extensive files,
-- ftp'able, Kermit, XYZmodems,

-- Died recently due to irreparable hardware failures. This system will probably remain down for a year or so, or indefinitely if another machine is not found for it. I will continue to update its status if any changes occur.

-- Mars is/was a Sparc 4/110 that lost a Mongo chip. The EE department might consider ordering a replacement, but has no idea where to get one. Information will be forwarded if sent to Zamfield@dune.ee.msstate.edu. Also, if anyone has a spare 4/110 the EE department said that would do just fine.

-- Further information, offerings, etc, contact Zamfield@dune.ee.msstate.edu and I will facilitate the rebirth of Mars if possible.

National Education BBS testsun3.nersc.gov bbs Pirate
-- shadowfax.nersc.gov
-- 128.55.128.183
-- 128.55.128.64

-- Boards, Talk, Chat, Mail.'source' file section, but no files. HAS GONE PRIVATE, or so I have been told. (9/22/91)

Netcom netcom.netcom.com guest + <CR> at passwd
-- 192.100.81.100

-- Full Unix service. Money for access. $15.50/month ($17.50 for invoiced billing)
-- (408) 241-9760/9794 (San Jose, CA) and
-- (415) 424-0131 (Palo Alto, CA).

Nyx BBS isis.cs.du.edu new
-- 130.253.192.9

-- Full news feed, Local downloads, shell access (with validation), and Ftp. It is a completely free public access Unix system fun by the University of Denver's Math and Computer Science Department.

-- Sysop: Professor. Andrew Burt. The system is run by donations on a donated Pyramid 90x with a homebrew menuing system

Olajier 129.31.22.7 Olajier <passwd Olajier>
-- leo.ee.ic.ac.uk

-- Capitals are important for both the login and passwd. This BBS is at Imperial College in London.

OuluBox (Finnish) tolsun.oulu.fi box
-- 130.231.96.16

-- Can set English as preferred language, said to switch to Finnish at the most inconvenient time. IRC.

The Picayune star96.nodak.edu 20
-- star24.nodak.edu or star12.nodak.edu for slower speeds.
-- 134.129.107.131

-- North Dakota Higher Education Computer Network.
-- Limited net news, file areas, tetris online, local e-mail.

-- A 386 running unix, 2 80 meg drives, 600 users give or take a few.

Quartz Quartz.Rutgers.Edu bbs Citadel
-- 128.6.60.6

-- Rooms/Boards.
-- Suggest MUD to chat.

Samba North Carolina 128.109.157.30 bbs Modified XBBS
-- samba.acs.unc.edu
-- (919)-962-9911

-- Offers vi, emacs, rn, NEWS, MAIL, local messaging, SIGS, Conferencing, Files (Kermit/FTP), & INFO limited NewsFeed (8/2/91).

Softwords COSY softwords.bc.ca cosy Cosy
-- 134.87.11.1

SpaceLink BBS spacelink.msfc.nasa.gov
-- 128.158.13.250

Spies In The Wires doomsday.spies.com bbs
-- 130.43.2.220

-- Full UseNet NewsFeed, Posting to UseNet.
-- IRC (for validated users).

-- Appears to have shut down. 12/6/91

TriState Online 129.137.100.1 visitor FreeNetIII
-- tso.uc.edu

-- new FreeNet site.

Virginia Tech Cosy vtcbx.csn.vt.edu cosyreg
-- 128.173.5.10 bbs (for list)

-- Virginia Tech Conferencing System. Offers local conferencing, up to date listing of local BBSes and read only Usenet NEWS. Tons of messages.

Youngstown Free-Net yfn.ysu.edu visitor
-- 192.55.234.27

Unknown centaur.ucsd.edu bbs
-- 128.54.16.14

The World world.std.com new
-- 192.74.137.5

-- Public access Unix system. 19.2, 9600, 2400, & 1200 baud modem connections. 3 GB disk storage. CompuServe Packet Network access and SLIP connection up to T1.

-- Signup, dial 617-739-WRLD, type new. Basic rates are $2/hr 24 hrs/day and $5 monthly fee. 20/20 plan, $20 for 20 hrs, including monthly fee. Also available from Compuserve Packet Network. $5.60 surcharge is added to monthly bill. Further info at staff@world.std.com

-- E-mail to Internet, UUCP, BITNET, CSNET, EUNET, JANET, JUNET, Fidonet, BIX, Compuserve, Applelink and MCImail.

-- USENET, ClariNet, Electronic Mailing Lists, Chatting, Unix Software, GNU Software, Games, Online Book Initiative, AlterNet Access, Internet.

- -

SERVICES
~~~~~~~~
The following is a list of useful services that most BBSers are interested in. I have not checked any of these except Archie. If you have more info about these or if you know of other to add, please mail me:

Zamfield@Dune.EE.MsState.EDU.

==========

Service Address Login

Archie quiche.cs.mcgill.ca archie
-- 132.206.2.3
~~~~~~~~

```
Cheeseplant's House 137.205.192.5 2001
 --  orchid.csv.warwick.ac.uk

 --  This is a dedicated Chat program run by Daniel Stephens in Warwick
     University in England.

Cat Chat  137.205.192.5 2000

 --  Another ChatServer.  See Cheeseplant's House.

DDN Network Information Center
 --  nic.ddn.mil
 --  192.67.67.20

 --  TACNEWS, WHOIS Server, NIC


GeoServer  Martini.eecs.umich.edu 3000
 --  141.212.100.9

IRC Client  bradenville.andrew.cmu.edu
 --  128.2.54.2

 --  not all IRC commands supported.

Library Systems  ->FTP<- vaxb.acs.unt.edu

 --  This site contains a huge, 100-150 page, guide to Internet libraries.
     The file is under the library directory.  Send thanks and responses to
     Billy Barron, BILLY@vaxb.acs.unt.EDU.

Lyric Server  ->FTP<- cs.uwp.edu

 --  These files are available via anonymous ftp.  This is not really a Telnet
     service, but it is nice to know about so I included it.

National Ham Radio Call-Sign Callbook
 --  128.205.32.4 2000
 --  marvin.cs.Buffalo.Edu

 --  I am very impressed with this service I heard that people had trouble
     logging into this site, but I never encountered a login prompt, I just
     started using it.

NCSU Services  ccvax1.cc.ncsu.edu INFO or PUBLIC
 --  128.109.153.4

Network Information Service (Univ. of California at Berkeley)
 --  mailhost.berkeley.edu 117
 --  128.32.136.9, 117
 --  128.32.136.12, 117
 --  128.32.206.9 117
 --  128.32.206.12 117

OCEANIC   128.175.24.1
 --  delocn.udel.edu

 --  Ocean info center, from the U. of Delaware.  Contains technical and
     scientific info on oceanic research.  DOS software for viewing
     oceanographic graphics.  Type <$> to logout (no brackets).

Slugnet chat system cons1.mit.edu
 --  18.80.0.88, 2727

 --  sorta like IRC.

UM-Weather Service madlab.sprl.umich.edu 3000
 --  141.212.196.79 3000
```

Vatech Server 128.173.16.6
-- vtcbx.cc.vt.edu

WAIS server hub.nnsc.nsf.net wais
-- 192.31.103.7

-- Gives access to online documents. More info can be obtained from THINK.COM.

Thomas A. Kreeger (Zamfield@Dune.EE.MsState.Edu)

---

nixpub short listing
Open Access UNIX (*NIX) Sites [both Fee and No Fee]
[September 13, 1991]

Legend: fee/contribution ($), no fee (-$), hours (24), not (-24)
shell (S), USENET news (N), e-mail (M), multiple lines (T)
Telebit PEP speed on main number (+P), Telebit on other line[s] (P)
Courier HST 9600 bps on main number (+H), Courier on other line[s] (H)
V.32 on main number (+V), V.32 on other line[s] (V)
anonymous uucp (A), archive site ONLY - see long form list (@)

Updated Last	Telephone #	Sys-name	Location		Baud	Legend
08/91	201-759-8450^	tronsbox	Belleville	NJ	3-96	24 -$ MN+PST
04/91	203-661-2873	admiral	Greenwich	CT	3/12/24/96	24 -$ AHMN+PT+V
09/91	206-328-4944^	polari	Seattle	WA	12	24 $ MNPST
05/91	206-367-3837^	eskimo	Seattle	WA	3/12/24	24 $ MNST
04/91	209-952-5347	quack	Stockton	CA	3/12/24/96	24 $ MN+PS
12/90	212-420-0527^	magpie	NYC	NY	3/12/24/96	24 -$ APT
12/90	212-431-1944^	dorsai	NYC	NY	3/12/24	24 $ MNT
12/90	212-675-7059^	marob	NYC	NY	3/12/24/96	24 -$ APT
12/90	213-397-3137^	stb	Santa Monica	CA	3/12/24/96	24 -$ A+PS
01/91	215-336-9503^	cellar	Philadelphia	PA	3/12/24/96	24 $ +HMN+V
06/91	215-348-9727	lgnp1	Doylestown	PA	3/12/24/96	24 -$ AMN+P
12/90	216-582-2460^	ncoast	Cleveland	OH	12/24/96	24 $ MNPST
07/91	217-789-7888	pallas	Springfield	IL	3/12/24/96	24 $ HMNSTV
07/91	219-289-0282	nstar	Notre Dame	IN	24/96	24 $ +HMNPST+V
08/91	301-625-0817	wb3ffv	Baltimore	MD	12/24/96	24 -$ AHNPT+V
07/91	303-871-4824^	nyx	Denver	CO	3/12/24	24 -$ MNST
08/91	312-248-0900	ddsw1	Chicago	IL	3/12/24/96	24 $ AMNPSTV
04/90	312-283-0559^	chinet	Chicago	IL	3/12/24/96	24 $ HNPT
10/89	312-338-0632^	point	Chicago	IL	3/12/24/96	24 -$ HNPST
09/90	312-714-8568^	gagme	Chicago	IL	12/24	24 $ MNS
06/90	313-623-6309	nucleus	Clarkston	MI	12/24	24 -$ AM
10/90	313-994-6333	m-net	Ann Arbor	MI	3/12/24	24 $ T
08/89	313-996-4644^	anet	Ann Arbor	MI	3/12	24 $ T
08/89	314-474-4581	gensis	Columbia	MO	3/12/24/48/	24 -$ MS
08/90	401-455-0347	anomaly	Esmond	RI	3/12/24/96	24 -$ MN+PS
09/91	407-299-3661^	vicstoy	Orlando	FL	12/24	24 -$ MNS
06/91	407-438-7138^	jwt	Orlando	FL	12/24/96	24 -$ MNP
11/90	408-241-9760^	netcom	San Jose	CA	12/24/96	24 $ MNPST
09/89	408-245-7726^	uuwest	Sunnyvale	CA	3/12/24	24 -$ N
08/91	408-423-9995	cruzio	Santa Cruz	CA	12/24	24 $ MNPT
07/91	408-458-2289	gorn	Santa Cruz	CA	3/12/24/96	24 -$ MN+PST
10/89	408-725-0561^	portal	Cupertino	CA	3/12/24	24 $ MNT
12/90	408-739-1520^	szebra	Sunnyvale	CA	3/12/24/96	24 -$ MN+P
07/91	408-867-7400^	spies	Saratoga	CA	12/24	24 -$ MNST
09/91	408-996-7358^	zorch	Cupertino	CA	12/24/96	24 $ MNPT
06/91	412-431-8649^	eklektik	Pittsburgh	PA	3/12/24	24 $ MNST
06/91	414-241-5469^	mixcom	Milwaukee	WI	12/24/96	24 $ MNST
09/91	414-734-2499	edsi	Appleton	WI	3/12/24	24 $ MN
01/91	415-223-9768^	barbage	El Sobrante	CA	3/12/24/48	24 -$
11/90	415-294-8591	woodowl	Livermore	CA	12/24/19.2	24 -$ MN+P
11/89	415-332-6106^	well	Sausalito	CA	12/24	24 $ MNST
06/91	415-623-8652^	jack	Fremont	CA	3/12/24/96	24 -$ MN+PST

06/91	415-826-0397^	wet	San Francisc	CA	12/24	24	$ MNPSTV
04/91	415-949-3133^	starnet	Los Altos	CA	3/12/24/96	24	$ MNPSTV
05/90	415-967-9443^	btr	Mountain Vie	CA	3/12/24	24	$ HMNPSTV
11/89	416-452-0926	telly	Brampton	ON	12/24/96	24	$ MN+P
12/88	416-461-2608	tmsoft	Toronto	ON	3/12/24/96	24	$ MNS
02/90	502-957-4200	disk	Louisville	KY	3/12/24	24	$ MNST
08/91	503-254-0458^	bucket	Portland	OR	3/12/24/96	24	-$ MN+PST+V
02/91	503-297-3211^	m2xenix	Portland	OR	3/12/24/96	24	-$ MN+PST+V
03/91	503-640-4262^	agora	PDX	OR	12/24/96	24	$ MNST
05/90	503-644-8135^	techbook	Portland	OR	12/24	24	$ MNST
09/91	508-655-3848	unixland	Natick	MA	12/24/96	24	$ HMNPSTV
06/91	512-346-2339^	bigtex	Austin	TX	96	24	-$ A+PS
10/89	513-779-8209	cinnet	Cincinnati	OH	12/24/96	24	$ MN+PS
08/90	514-844-9179	tnl	Montreal	PQ	3/12/24	24	-$ MS
01/90	517-487-3356	lunapark	E. Lansing	MI	12/24	24	-$
12/88	518-346-8033	sixhub	upstate	NY	3/12/24	24	$ MNST
07/91	602-293-3726	coyote	Tucson	AZ	3/12/24/96	24	-$ MN+P
07/91	602-649-9099^	telesys	Mesa	AZ	12/24/96	24	$ AMN+PS
12/90	602-941-2005^	xroads	Phoenix	AZ	12/24	24	$ NT
11/90	604-576-1214	mindlink	Vancouver	BC	3/12/24/96	24	$ HMNPT
12/90	604-753-9960	oneb	Nanaimo	BC	3/12/24/96	24	$ MN+PT
08/89	605-348-2738	loft386	Rapid City	SD	3/12/24/96	24	$ MN+PS
04/91	606-263-5106	lunatix	Lexington	KY	3/12/24	24	-$ MNST
08/88	608-273-2657	madnix	Madison	WI	3/12/24	24	-$ MNS
09/90	612-473-2295^	pnet51	Minneapolis	MN	3/12/24	24	-$ MNT
12/90	613-237-0792	latour	Ottawa	ON	3/12/24/96	24	-$ AMN+PS+V
12/90	613-237-5077	micor	Ottawa	ON	3/12/24/96	24	-$ MN+P
06/91	614-868-9980^	bluemoon	Reynoldsburg	OH	3/12/24/96	24	-$ +HMNPT
07/91	615-288-3957	medsys	Kingsport	TN	12/24/96	24	-$ AN+P
04/91	615-896-8716	raider	Murfreesboro	TN	12/24/96	24	-$ MNST+V
11/90	616-457-1964	wybbs	Jenison	MI	3/12/24/96	24	-$ MN+PST
06/91	617-471-9675^	fcsys	Quincy	MA	3/12/24/96	24	-$ AMN+V
12/90	617-739-9753^	world	Brookline	MA	3/12/24/96	24	$ MNPST
01/90	619-259-7757	pnet12	Del Mar	CA	3/12/24/96	24	-$ MNPT
07/88	619-444-7006^	pnet01	El Cajon	CA	3/12/24	24	$ MNST
06/91	703-239-8993^	tnc	Fairfax Stat	VA	3/12/24/96	24	-$ MNPT
12/89	703-281-7997^	grebyn	Vienna	VA	3/12/24	24	$ MNT
05/91	708-833-8126^	vpnet	Villa Park	IL	12/24/96	24	-$ MN+PST
06/91	713-438-5018^	sugar	Houston	TX	3/12/24/96	24	-$ N+PT
08/91	713-568-0480^	taronga	Hoston	TX	3/12/24	24	-$ MNST
10/89	713-668-7176^	nuchat	Houston	TX	3/12/24/96	24	-$ MN+PS
04/91	714-278-0862	alchemy	Corona	CA	12/24/96	24	-$ MN+PS
01/91	714-635-2863^	dhw68k	Anaheim	CA	12/24/96	24	-$ MN+PST
12/90	714-821-9671^	alphacm	Cypress	CA	12/24/96	24	-$ A+PT
12/90	714-842-5851^	conexch	Santa Ana	CA	3/12/24	24	$ AMNS
01/91	714-894-2246^	stanton	Irvine	CA	3/12/24	24	$ MNS
03/90	717-657-4997	compnect	Harrisburg	PA	3/12/24	24	-$ MNT
06/91	718-424-4183^	mpoint	New York	NY	3/12/24/96	24	$ +HMNS+V
04/91	718-832-1525^	panix	New York Cit	NY	12/24/96	24	$ MNPST
12/89	719-632-4111	oldcolo	Colo Spgs	CO	12/24/96	24	$ HMNT
12/90	808-735-5013	pegasus	Honolulu	HI	12/24/96/19	24	-$ MN+PST+V
12/90	812-333-0450	sir-alan	Bloominingto	IN	12/24/19.2/	24	-$ A+HMPTV
08/91	812-421-8523	aquila	Evansville	IN	12/24	24	$ AM
06/91	818-401-9611^	abode	El Monte	CA	24/96	24	$ MN+PST
03/91	900-468-7727	uunet	Falls Church	VA	3/12/24/96	24	$ AMN+PT+V
07/91	904-456-2003	amaranth	Pensacola	FL	12/24/96	24	-$ MN+P
09/91	906-228-4399	lopez	Marquette	MI	12/24	24	$ MN
06/91	908-297-8713^	kb2ear	Kendall Park	NJ	3/12/24/96	24	-$ AMNS+V
05/90	908-846-2460^	althea	New Brunswic	NJ	3/12/24	24	-$ MNS
08/91	916-649-0161^	sactoh0	Sacramento	CA	12/24/96	24	$ MN+PSTV
01/91	919-248-1177^	rock	RTP	NC	3/12/24/96	24	$ MN
10/89	919-493-7111^	wolves	Durham	NC	3/12/24	24	$ MNS
08/91	+33-1-40-35-23-49	gna	Paris	FR	12	24	-$ AMN+PT+V
11/90	+39-541-27858	xtc	Rimini (Fo)	IT	3/12/24/96	24	-$ HN+PT
09/91	+41-61-8115492	ixgch	Kaiseraugst	CH	3/12/24	24	-$ AMN+P
02/91	+44-81-853-3965	dircon	London	UK	3/12/24	24	$ MN
11/90	+44-81-863-6646	ibmpcug	Middlesex	UK	3/12/24/96	24	$ MST+V
06/91	+49-30-691-95-20	scuzzy	Berlin	DE	3/12/24/96	24	-$ A+HS
06/91	+49-8106-34593	gold	Baldham	DE	3/12/24/96	24	-$ AHMN+PT+V
01/91	+64-4-642-260	cavebbs	Wellington	NZ	12/24	24	-$ MNT

```
11/90  +64-4-895-478      actrix    Wellington   NZ 3/12/24/96  24 $ +HMNST
02/91  +64-9-645-593      delphi    Auckland     NZ 3/12/24/96  24 -$ MNT+V
02/91  +64-9-817-3725     kcbbs     Auckland     NZ 12/24/96    24 -$ MN+PTV

NOTE:  ^ means the site is reachable using PC Pursuit.
```

==Phrack Inc.==

Volume Four, Issue Thirty-Eight, File 6 of 15

BEATING THE RADAR RAP

Part 2 of 2 : "The Technical Side"

by Dispater

Introduction

Welcome to the second installment in this series where we will briefly explore some of the technical sides to the operations, error analysis of the police traffic RADAR unit, the basics of how this technology was developed, then how it was implemented, a list of common RADAR errors, and finally the technical analysis of various types of traffic RADAR by National Highway Safety Administration.

RADAR stands for Radio Detecting And Ranging. A traffic speed RADAR works under the principle of physicals called the "Doppler effect." This theory means that when a signal is reflected off of an object moving toward you, the signal will be at a higher frequency when it is closer to you than when the object is farther away or at the initial position. So the "Doppler effect" is THE basis for the use of the traffic speed RADAR.

Right now in the United States, there are three bands that are allocated by the Federal Communications Commission (FCC) for "field disturbance sensors." These three bands have non-technical names, and all operate in the GigaHertz range (GigaHertz is a measure of frequency, i.e. 1 GHz = 1 billion cycles per second). The following is a list of the RADAR bands (as a point of reference FM radio modulates at 0.088 GHz to 0.108 GHz).

BAND	FREQUENCY	NOTE ABOUT SPECIFIC BAND
X-Band	10.525 GHz	This is the frequency in which most RADAR units operate.
K-Band	24.150 GHz	K-Band was developed to give a longer range of the beam.
Ka-Band	26.450 GHz	This bandwidth is primarily for use with RADAR units that are used for "photo-speed traps."

"So if RADAR is so unreliable," you ask, "why don't we have planes crashing on a daily basis?" In the first place, TRAFFIC RADAR operates on a COMPLETELY different basis than, say, the type of RADAR that tracks weather or airplanes.

The technology of traffic RADAR can in no way be compared to the accuracy of other types of RADAR. Traffic RADAR does NOT "sweep" like a regular RADAR. "Sweeping" means that the RADAR is picking up every single return signal it gets and plots them proportionally on a two-dimensional cathode ray tube. On the other hand, traffic RADAR uses a stationary beam. Also, traffic RADAR does not use a modulated beam like regular RADAR; it uses a constant beam. ***This is an important distinction because this means that if there are multiple images, the constant RADAR beam cannot distinguish between them!***

Furthermore, traffic RADAR is limited to things such as size. It must be able to fit inside a patrol car and it is also subject to cost. That means a municipality usually picks up the lowest bid it can get from various manufacturers.

Implementation of Traffic RADAR

It is important to note at this time that while government standards for accuracy for military and commercial airline RADAR exist, traffic RADAR is NOT subject to ANY government standards whatsoever. An attempt was made to do this by the police and two government agencies, but were refused any type of compliance with traffic speed RADAR manufacturers and the Reagan administration.

In the late 1970s, there was wide-spread publicity of about RADAR errors, including the well known tree clocked at 86-MPH in Florida. So, in 1979 the

National Highway Safety Administration (NHSA) assigned to the National Bureau of Standards the task of testing all brands of traffic RADAR in use at that time for the purpose of discovering the source of these errors and proposing federal standards to eliminate them. In January of 1981, the proposed standards were published in the Federal Register. However, the Reagan administration took no action on the proposal (the last part of this file contains the profile from this report of various RADAR units).

After THREE years of government inaction on the problem, the International Association of the Chief of Police (IACP) provided non-government standards by which all traffic RADAR units could be tested to assure accuracy: Volume I of the standards was published in April, 1984 and Volume II in June, of 1984.

In June of 1986, the traffic RADAR manufacturers announced the formation of their own trade association, saying that they would not submit traffic RADAR units for IACP testing! Instead, they said they would use their own standards.

So far, NO ONE has any idea of what these standards are; not the police, not the government and, most importantly, not the public! Basically, there are no performance requirements or standards for traffic RADAR and the claims of 86-MPH trees and 28-MPH houses cannot be refuted.

Common Traffic Radar Errors

Below is a list of common errors and how they occur. This is the part of the article that must be used in conjunction with the previous file in this series. You must attempt, while pleading your case, to tie in some of the following errors to the situation you found yourself in when you got your speeding ticket. See Phrack #37 file #5 for details.

"The Look-Past Error" Even when the RADAR operator aims his gun properly, the RADAR is subject to this type of error. This is caused by the RADAR reflecting off of a larger surface area in the background rather than the smaller reflective surface in the foreground. Evidence of this the Look-Past Error was printed in the October 1979 issue of "Car and Driver." The author measured the effectiveness of KR11 RADAR system against various vehicles. The author showed that the typical sedan did not show up on the RADAR until it was less that 1200 feet away, however, a Ford 9000 semi tractor trailer could be picked up at 7600 feet.

"The Road Sign Error" Due to the reflectability of microwaves, road signs, buildings, billboards, large trees, and other stationary objects are a source of errors.

"Radio Interference Error" According to the Texas Department of Public Safety, "UHF frequencies broadcast today can force RADAR to read various numbers when transmitted within the area." This type of interference could come from the radio within the patrol car, citizens band radio, or television stations.

"Fan Interference Error" When the antenna is mounted inside the patrol car, "RADAR will have the tendency to read the pulse of the fan motor (air conditioner, heater, defroster)." This is a statement provided by the Texas Department of Public Safety who conducted a study of RADAR guns in 1987. The Texas Department of Public Safety offered no safeguard for this error.

"Beam Reflection Error" Since microwaves are so readily reflected, the Texas Department of Public Safety cautioned mounting the antenna within the patrol car. One instructor said, "It is possible that a reflective path can be set up through the rear view mirror that will produce RADAR readings on the vehicles behind the patrol car when the RADAR is aimed forward. And those vehicles can be either coming or going since traffic RADAR cannot distinguish between the direction."

"Double Bounce Error" Again, since microwaves are easily reflected, the operator must be aware of a "bad bounce" and an ordinary reflection. And, as stated before, since large objects are more efficient than smaller ones, microwaves are attracted to them more. So, in effect, you could have an initial RADAR bounce off of the target vehicle, then from the target vehicle to a house or a truck going the opposite direction, and finally back to the patrol

car. This error will mathematically get larger the slower the target vehicle is moving.

"The Cosine Error" This is a mathematical error that takes place when the RADAR gun attempts to calculate the trigonomic equation that is programmed into it. The RADAR gun measures the angle at which the target enters a point and then exits a point (i.e. 25 degrees). The cosine of 25 is .9063. The RADAR gun was designed to calculate the speed of the patrol car by multiplying the speed of the patrol car (i.e. 50 mph) and the cosine of the angle (.9063) and it gets the false speed of the patrol vehicle as 45mph. Therefore, when you subtract the patrol speed from the target speed (i.e. 50, the same as the patrol car) you get the false sense that the target vehicle is traveling 5mph faster than the patrol car.

Technical Analysis Report

Below is a copy of the report mentioned above was conducted by the NHSA. But first I will explain what some of the criteria were under the testing conditions. It is also important to note that ALL RADAR units were subject to "panning error" except the CMI Speedgun-6 and Speedgun-8 models. Panning error occurs when the RADAR antenna is aimed at it's own display console. Unintentional errors of this sort can be eliminated when police officers are given adequate training.

TEST UNIT : Model and manufacturer of the police speed RADAR unit in question.

BAND : The short hand used for determining the broadcast frequency of the RADAR unit. X-Band is 8.2-12.4 GHz. K-Band is 18.0-26.5 GHz.

BEAM WIDTH : The number that is 1/2 of the actual beam width. In other words, if a RADAR manufacturer says the beam width is 24 degrees, the actual beam width is 48 degrees. Very deceptive, eh?

SHADOWING ERROR : This occurs in moving mode only. It is the result of the RADAR mistaking another vehicle for it's ground reference and adding speed to the target reading.

POWER SURGE : This occurs when the RADAR unit is first turned on. This also occurs when the "kill switch" is used to defeat RADAR detectors. Lag time for kill in the moving mode ranges from 1.5-5 seconds.

EXTERNAL INTERFERENCE : The NBS test only used CB radio and police-band radio for "external interference." There are many other kinds of outside electromagnetic interference that may effect police RADAR.

INTERNAL INTERFERENCE : Internal interference "may be caused by ANY electrical component or accessory in the vehicle, especially when the patrol car's primary power source is used to operate the RADAR.

[It should be noted that TWO of MPH's K-55 RADAR units were tested. This demonstrates that each RADAR unit can contain its own quirks regardless of the fact that it can be from the same model from the same manufacturer.]

NATIONAL BUREAU OF STANDARDS SUMMARY ON TRAFFIC RADAR

TEST UNIT	BAND	BEAM WIDTH	SHADOWING ERROR
Kustom Signals MR-9	K	13.3	Minor

POWER SURGE	EXTERNAL INTERF.	INTERNAL INTERF.
Switch-ON gave stray reading of 7mph	CB radio caused false readings of up to 25’	CB radio caused erroneous readings

TEST UNIT	BAND	BEAM WIDTH	SHADOWING ERROR
MPH Industries K-55 (first of two units)	X	20.4	Added 12mph to target in one test

POWER SURGE	EXTERNAL INTERF.	INTERNAL INTERF.
No valid reading for 2.4 sec in moving mode	CB radio caused false readings of up to 20’	CB radio many erroneous readings

TEST UNIT	BAND	BEAM WIDTH	SHADOWING ERROR
MPH Industries K-55 (second of two units)	X	24.6	Increased target speed 12-15mph about 20% of the time

POWER SURGE	EXTERNAL INTERF.	INTERNAL INTERF.
2 sec delay in moving mode, 2.5 sec in stationary mode	CB radio caused false alarms up to 175’ away	CB radio cause many erroneous readings

TEST UNIT	BAND	BEAM WIDTH	SHADOWING ERROR
Decatur MV-715	X	17.5	Added 8-23mph to target in repeated testing

POWER SURGE	EXTERNAL INTERF.	INTERNAL INTERF.
No valid reading for 2+ seconds in moving mode	Not effected by external CB radio	Extreme interference from heater fan, ignition, & CB radio

TEST UNIT	BAND	BEAM WIDTH	SHADOWING ERROR
CMI Speedgun-6	X	18.8	Very severe, added 12-20 mph to target

POWER SURGE	EXTERNAL INTERF.	INTERNAL INTERF.
7 sec delay in moving mode, 2 sec delay in stationary	Not effected by external CB radio	CB radio and police radio boosts readings 20mph

TEST UNIT	BAND	BEAM WIDTH	SHADOWING ERROR
CMI Speedgun-8	X	18.6	target traveling 41mph shown as 74mph; target 30mph shown as 41mph

POWER SURGE	EXTERNAL INTERF.	INTERNAL INTERF.
2 sec delay in moving mode, 1.2 sec delay in stationary	Not effected by external CB radio	No adverse effect noted

TEST UNIT	BAND	BEAM WIDTH	SHADOWING ERROR

Kustom Signals MR-7	X	14.3	No effects noted

POWER SURGE	EXTERNAL INTERF.	INTERNAL INTERF.
25.4 sec delay in moving mode, 0.6 sec delay in stationary	Not effected by external CB radio	Police band radio caused intermittent increases of 10mph

In Closing...

I hope you have learned a little about how police speed RADAR operates, the errors that they frequently incur, and possibly a way to avoid the highway robbery that occurs each time Officer Friendly decides to make a little extra dough for his "job security."

Also, if you are interested in obtaining cheap traffic RADAR equipment to play with, you can write to: AIS SATELLITE INC., 106 N. Seventh Street, Perkasie, PA 18944. You can also call them for a catalog at (215)453-1400 or place orders at (800)AIS-2001.

== Phrack Inc. ==

Volume Four, Issue Thirty-Eight, File 7 of 15

```
      <:=--=:><:=--=:><:=--=:><:=--=:>\|/<:=--=:><:=--=:><:=--=:><:=--=:>
      <:=--=:>                                                     <:=--=:>
      <:=--=:>    >>>>>=-*  Users Guide to VAX/VMS  *-=<<<<<     <:=--=:>
      <:=--=:>                                                     <:=--=:>
      <:=--=:>                  Part III of III                    <:=--=:>
      <:=--=:>                                                     <:=--=:>
      <:=--=:>           Part E: DCL Command Reference             <:=--=:>
      <:=--=:>         Part F: Lexical Function Reference          <:=--=:>
      <:=--=:>                                                     <:=--=:>
      <:=--=:>                    By Black Kat                     <:=--=:>
      <:=--=:>                                                     <:=--=:>
      <:=--=:><:=--=:><:=--=:><:=--=:>/|\<:=--=:><:=--=:><:=--=:><:=--=:>
```

Index

<:=- Part E : DCL Command Reference -=:>

DCL Command Reference

@ file_spec [p1 p2...p8]
  Executes a DCL command procedure.

  Qualifier:
  /OUTPUT=file_spec

ACCOUNTING file_spec[,...]
  Invokes the VAX/VMS Accounting Utility to collect and report accounting
  information.

  Qualifiers:

/ACCOUNT	/ADDRESS	/BEFORE	/BINARY	/ENTRY
/FULL	/IDENTIFICATION	/IMAGE	/JOB	/LOG
/NODE	/OUTPUT	/OWNER	/PRIORITY	/PROCESS
/QUEUE	/REJECTED	/REMOTE_ID	/REPORT	/SINCE
/SORT	/STATUS	/SUMMARY	/TERMINAL	/TITLE
/TYPE	/UIC	/USER		

ALLOCATE device_name: [logical_name]
  Provides exclusive use of a device and, optionally, establishes a logical
  name for that device. While a device is allocated, other users may access
  the device until you DEALLOCATE it or log out.

  Qualifier:
  /GENERIC

ANALYZE
  Invokes various VAX/VMS utilities to examine components of the system. The
  default function is to examine a module (ANALYZE/OBJECT).

  Qualifiers:

/CRASH_DUMP	/DISK_STRUCTURE	/ERROR_LOG	/IMAGE
/MEDIA	/OBJECT	/PROCESS_DUMP	/RMS_FILE
/SYSTEM			

APPEND input_file_spec[,...] output_file_spec
  Adds the contents of one or more input files to the end of a file.

```
  Qualifiers:
  /ALLOCATION    /BACKUP       /BEFORE         /BY_OWNER       /CONFIRM
  /CONTIGUOUS    /CREATED      /EXCLUDE        /EXPIRED        /EXTENSION
  /LOG           /MODIFIED     /NEW_VERSION    /READ_CHECK     /SINCE
  /WRITE_CHECK


ASSIGN
  Equates a logical name to a physical device name, file specification or
  another logical name.


ASSIGN/MERGE
  Merges the contents of one queue with another.


ASSIGN/QUEUE
  Assigns a logical queue to a device queue.


ATTACH [process_name]
  Enables you to transfer control from the current process to another process
  created by you (see SPAWN).

  Qualifier:
  /IDENTIFICATION


BACKUP input_spec output_spec
  Invokes the VAX/VMS Backup Utility to perform one of the following file
  operations:
  o  Copy disk files.
  o  Save disk files as a save set (a single data file) on a disk or
     magnetic tape volume.
  o  Restore files from a save set.
  o  Compare files.
  o  Display information about files contained in a save set.

  Qualifiers:
  /BACKUP          /BEFORE         /BLOCK_SIZE     /BRIEF
  /BUFFER_COUNT    /COMMENT        /COMPARE        /CONFIRM
  /CRC             /CREATED        /DELETE         /DENSITY
  /EXCLUDE         /EXPIRED        /FAST           /FULL
  /GROUP_SIZE      /IGNORE         /IMAGE          /INCREMENTAL
  /INITIALIZE      /INTERCHANGE    /JOURNAL        /LABEL
  /LIST            /LOG            /MODIFIED       /NEW_VERSION
  /OVERLAY         /OWNER_UIC      /PHYSICAL       /PROTECTION
  /RECORD          /REPLACE        /REWIND         /SAVE_SET
  /SELECT          /SINCE          /TRUNCATE       /VERIFY
  /VOLUME


CALL label [p1 p2...p8]
  Transfers command procedure control to a labeled subroutine in the procedure.

  Qualifier:
  /OUTPUT


CANCEL [process_name]
  Cancels a scheduled wake_up request for the specified process.

  Qualifier:
  /IDENTIFICATION


CLOSE logical_name
  Closes a file opened for input/output with the OPEN command, and deassigns
  the logical name created for the file.
```

```
  Qualifiers:
  /ERROR        /LOG


CONNECT virtual_terminal_name
  Connects a physical terminal to a virtual terminal connected to another
  process.

  Qualifiers:
  /CONTINUE     /LOGOUT


CONTINUE
  Resumes execution of a DCL command, program or command procedure
  interrupted by pressing <Ctrl-Y> or <Ctrl-C>.  You can abbreviate the
  CONTINUE command to the letter C.


COPY input_file_spec[,...] output_file_spec
  Creates a new file from one or more existing files.  The COPY command can be
  used to:
  o  Copy an input file to an output file, optionally changing its name and
     location.
  o  Copy a group of input files to a group of output files.
  o  Concatenate two or more files into a single new file.

  Qualifiers:
  /ALLOCATION     /BACKUP        /BEFORE       /BY_OWNER     /CONCATENATE
  /CONFIRM        /CONTIGUOUS    /CREATED      /EXCLUDE      /EXPIRED
  /EXTENSION      /LOG           /MODIFIED     /OVERLAY      /PROTECTION
  /READ_CHECK     /REPLACE       /SINCE        /TRUNCATE     /VOLUME
  /WRITE_CHECK


CREATE file_spec
  Creates one or more sequential disk files from records that follow in the
  input stream (i.e., the keyboard, a modem...).  To terminate input and close
  the file, enter <Ctrl-Z>.

  Qualifiers:
  /LOG          /OWNER_UIC      /PROTECTION     /VOLUME


CREATE/DIRECTORY directory_spec[,...]
  Creates a new directory or subdirectory for cataloging files.

  Qualifiers:
  /LOG      /OWNER_UIC     /PROTECTION     /VERSION_LIMIT    /VOLUME


CREATE/FDL=fdl_file_spec [file_spec]
  Invokes the FDL (File Definition Language) Utility to use the
  specifications in a definition file to create a new (empty) data file.

  Qualifier:
  /LOG


DEALLOCATE device_name:
  Releases a previously allocated device to the pool of available devices.

  Qualifiers:
  /ALL


DEASSIGN logical_name[:]
  Deletes logical name assignments made with the ALLOCATE, ASSIGN, DEFINE, or
  MOUNT command.
```

```
  Qualifiers:
  /ALL          /EXECUTE_MODE          /GROUP          /JOB
  /PROCESS      /SUPERVISOR_MODE       /SYSTEM         /TABLE
  /USER_MODE


DEASSIGN/QUEUE logical_queue_name[:]
  Deassigns a logical queue from its printer or terminal queue assignment and
  stops the associated logical queue.


DEBUG
  Invokes the VAX/VMS Debugger.


DEFINE logical_name equivalence_name[,...]
  Creates a logical name entry and assigns it an equivalence string, or a list
  of equivalence strings, to the specified logical name.

  Qualifiers:
  /EXECUTIVE_MODE             /GROUP                /JOB
  /LOG                        /NAME_ATTRIBUTES      /PROCESS
  /SUPERVISOR_MODE            /SYSTEM               /TABLE
  /TRANSLATION_ATTRIBUTES     /USER_MODE            /CHARACTERISTIC
  /FORM                       /KEY


DEFINE/KEY key_name string
  Associates a character string and a set of attributes with a function key.

  Qualifiers:
  /ECHO         /ERASE          /IF_STATE       /LOCK_STATE     /LOG
  /SET_STATE    /TERMINATE


DELETE file_spec[,...]
  Deletes one or more files from a mass device.

  Qualifiers:
  /BACKUP     /BEFORE      /BY_OWNER     /CONFIRM    /CREATED
  /ERASE      /EXCLUDE     /EXPIRED      /LOG        /MODIFIED
  /SINCE


DELETE/CHARACTERISTIC characteristic_name
  Deletes the definition of a queue characteristic that previously was
  established with the DEFINE/CHARACTERISTIC command.


DELETE/ENTRY=(queue_entry_number[,...]) queue_name[:]
  Deletes one or more job entries from the named queue.


DELETE/KEY key_name
  Deletes a key definition established by the DEFINE/KEY command.

  Qualifiers:
  /ALL        /LOG        /STATE


DELETE/QUEUE queue_name[:]
  Deletes the specified queue from the system.


DELETE/SYMBOL symbol_name
  Removes a symbol definition from a local or global symbol table or removes
  all symbol definitions in a symbol table.

  Qualifiers:
  /ALL       /GLOBAL       /LOCAL        /LOG
```

```
DEPOSIT location=data[,...]
  Over-writes the contents of a specified location or series of locations in
  virtual memory.  The DEPOSIT and EXAMINE commands are used (mostly) while
  debugging programs interactively.

  Qualifiers:
  /ASCII        /BYTE     /DECIMAL      /HEXADECIMAL
  /LONGWORD     /OCTAL    /WORD


DIFFERENCES master_file_spec [revision_file_spec]
  Compares the contents of two disk files and creates a listing of those
  records that do not match.

  Qualifiers:
  /CHANGE_BAR   /COMMENT_DELIMITER      /IGNORE
  /MATCH        /MAXIMUM_DIFFERENCES    /MERGED
  /MODE         /NUMBER                 /OUTPUT
  /PARALLEL     /SEPARATED              /SLP
  /WIDTH        /WINDOW


DIRECTORY [file_spec[,...]]
  Provides a list of files or information about a file or group of files.

  Qualifiers:
  /ACL          /BACKUP     /BEFORE         /BRIEF         /BY_OWNER
  /COLUMNS      /CREATED    /DATE           /EXCLUDE       /EXPIRED
  /FILE_ID      /FULL       /GRAND_TOTAL    /HEADING       /MODIFIED
  /OUTPUT       /OWNER      /PRINTER        /PROTECTION    /SECURITY
  /SELECT       /SINCE      /SIZE           /TOTAL         /TRAILING
  /VERSIONS     /WIDTH


DISCONNECT
  Disconnects a physical terminal from a virtual terminal that has been
  connected to a process.  The virtual terminal, and its associated process
  will remain on the system when the physical terminal is disconnected from it.

  Qualifier:
  /CONTINUE


DISMOUNT device_name[:]
  Dismounts a disk or magnetic tape volume that previously was mounted with a
  MOUNT command.

  Qualifiers:
  /ABORT      /CLUSTER      /UNIT     /UNLOAD


DUMP file_spec[,...]
  Displays the contents of files or volumes in ASCII, decimal, hexadecimal or
  octal representation.

  Qualifiers:
  /ALLOCATED     /BLOCKS     /BYTE           /DECIMAL      /FILE_HEADER
  /FORMATTED     /HEADER     /HEXADECIMAL    /LONGWORD     /NUMBER
  /OCTAL         /OUTPUT     /PRINTER        /RECORDS      /WORD


EDIT/ACL file_spec
  Invokes the Access Control List Editor to create or update access control
  list information for a specified object.

  Qualifiers:
  /JOURNAL      /KEEP     /MODE      /OBJECT     /RECOVER
```

```
EDIT/EDT file_spec
  Invokes the VAX/VMS EDT text editor.  The /EDT qualifier is not required, as
  EDT is the default editor.

  Qualifiers:
  /COMMAND      /CREATE      /JOURNAL     /OUTPUT     /READ_ONLY
  /RECOVER


EDIT/FDL file_spec
  Invokes the VAX/VMS FDL (File Definition Language) Editor to create or modify
  File and FDL files.

  Qualifiers:
  /ANALYSIS       /CREATE           /DISPLAY        /EMPHASIS
  /GRANULARITY    /NOINTERACTIVE    /NUMBER_KEYS    /OUTPUT
  /PROMPTING      /RESPONSES        /SCRIPT


EDIT/TPU file_spec
  Invokes the VAX/VMS Text Processing Utility.  The EVE (Extensible VAX Editor)
  is the default interface for TPU.  To invoke TPU with the EDT emulator
  interface, define the logical TPUSECII to point to the section file for the
  EDT interface as follows:
  $ DEFINE  TPUSECINI  EDTSECINI

  Qualifiers:
  /COMMAND      /CREATE         /DISPLAY        /JOURNAL
  /OUTPUT       /READ_ONLY      /RECOVER        /SECTION


EOD
  Signals the end of an input stream when a command, program or utility is
  reading data from an input device other than a terminal.


EXAMINE location[:location]
  Displays the contents of virtual memory.

  Qualifiers:
  /ASCII        /BYTE        /DECIMAL       /HEXADECIMAL
  /LONGWORD     /OCTAL       /WORD


EXIT [status_code]
  Terminates the current command procedure.  If the command procedure was
  executed from within another command procedure, control will return to the
  calling procedure.


GOSUB label
  Transfers command procedure control to a labeled subroutine.


GOTO label
  Transfers control to a labeled statement in a command procedure.


HELP
  Invokes the VAX/VMS Help Utility to display information about a VMS command
  or topic.

  Qualifiers:
  /INSTRUCTIONS         /LIBLIST        /LIBRARY        /OUTPUT
  /PAGE                 /PROMPT         /USERLIBRARY


IF logical_expression THEN dcl_command
  Tests the value of a logical expression and executes the command following
```

the THEN keyword if the test is true.

INITIALIZE device_name[:] volume_label
Formats and writes a label on a mass storage volume.

Qualifiers:

/ACCESSED	/BADBLOCKS	/CLUSTER_SIZE	/DATA_CHECK
/DENSITY	/DIRECTORIES	/ERASE	/EXTENSION
/FILE_PROTECTION	/GROUP	/HEADERS	/HIGHWATER
/INDEX	/LABEL	/MAXIMUM_FILES	/OVERRIDE
/OWNER_UC	/PROTECTION	/SHARE	/STRUCTURE
/SYSTEM	/USER_NAME	/VERIFIED	/WINDOWS

INITIALIZE/QUEUE queue_name[:]
Creates and initializes queues. This command is used to create and assign names and attributes to queues. When creating a batch queue, the qualifier /BATCH is required.

Qualifiers:

/BASE_PRIORITY	/BATCH	/BLOCK_LMIT	/CHARACTERISTICS
/CPUDEFAULT	/CPUMAXIMUM	/DEFAULT	/DISABLE_SWAPPING
/ENABLE_GENERIC	/FORM_MOUNTED	/GENERIC	/JOB_LIMIT
/LIBRARY	/ON	/OWNER_UIC	/PROCESSOR
/PROTECTION	/RECORD_BLOCKING	/RETAIN	/SCHEDULE
/SEPARATE	/START	/TERMINAL	/WSDEFAULT
/WSEXTENT	/WSQUOTA		

INQUIRE symbol_name [prompt]
Provides interactive assignment of a value for a local or global symbol in a command procedure.

Qualifiers:

/GLOBAL	/LOCAL	/PUNCTUATION

LIBRARY library_file_spec [input_file_spec[,...]]
Invokes the VAX/VMS Librarian Utility to create, modify, or describe a macro, object, help, text or shareable image library.

Qualifiers:

/BEFORE	/COMPRESS	/CREATE	/CROSS_REFERENCE
/DATA	/DELETE	/EXTRACT	/FULL
/GLOBALS	/HELP	/HISTORY	/INSERT
/LIST	/LOG	/MACRO	/NAMES
/OBJECT	/ONLY	/OUTPUT	/REMOVE
/REPLACE	/SELECTIVE_SEARCH	/SHARE	/SINCE
/SQUEEZE	/TEXT	/WIDTH	/MODULE

LINK file_spec[,...]
Invokes the VAX/VMS Linker to link object modules into a VMS program image.

Qualifiers:

/BRIEF	/CONTIGUOUS	/CROSS_REFERENCE	/DEBUG
/EXECUTABLE	/FULL	/HEADER	/MAP
/IMAGE	/PROTECT	/SHAREABLE	/SYMBOL_TABLE
/SYSLIB	/SYSSHR	/SYSTEM	/TRACEBACK
/USERLIBRARY	/INCLUDE	/LIBRARY	/OPTIONS
/SELECTIVE_SEARCH	/SHAREABLE		

LOGOUT
Terminates an interactive terminal session with VMS.

Qualifiers:

/BRIEF	/FULL	/HANGUP

```
MACRO file_spec[,...]
  Invokes the VAX/VMS MACRO assembler to assemble MACRO assembly language
  source programs.

  Qualifiers:
  /CROSS_REFERENCE      /DEBUG          /DISABLE        /ENABLE
  /LIBRARY              /LIST           /OBJECT         /SHOW
  /UPDATE


MAIL [file_spec] [recipient_name]
  Invokes the VAX/VMS Personal Mail Utility, which is used to send messages to,
  and receive messages from, other users of the system.

  Qualifiers:
  /SUBJECT      /EDIT     /SELF


MERGE input_file_spec1,input_file_spec2[,...] output_file_spec
  Invokes the VAX/VMS Sort Utility to combine up to 10 similarly sorted input
  files.  The input files to be merged must be in sorted order before invoking
  MERGE.

  Qualifiers:
  /CHECK_SEQUENCE       /COLLATING_SEQUENCE     /DUPLICATES
  /KEY                  /SPECIFICATION          /STABLE
  /STATISTICS           /FORMAT                 /ALLOCATION
  /BUCKET_SIZE          /CONTIGUOUS             /FORMAT
  /INDEXED_SEQUENTIAL   /OVERLAY                /RELATIVE
  /SEQUENTIAL


MESSAGE file_spec[,...]
  Invokes the VAX/VMS Message Utility to compile message definition files.

  Qualifiers:
  /FILE_NAME    /LIST   /OBJECT    /SYMBOLS     /TEXT


MONITOR [class_name[,...]]
  Invokes the VAX/VMS Monitor Utility to monitor various classes of system
  performance data.  Data can be analyzed from a running system or from a
  previously created recording file.  You can execute a single MONITOR request,
  or enter MONITOR interactive mode to execute a number of requests.  The
  interactive mode is entered by entering the MONITOR command with no
  parameters or qualifiers.  A MONITOR request is terminated by entering
  <Ctrl-C> or <Ctrl-Z>.  Pressing <Ctrl-C> causes MONITOR to enter interactive
  mode, while <Ctrl-Z> returns control to DCL.

  Parameters:
  ALL_CLASSES           CLUSTER         DECNET
  DISK                  DLOCK           FCP
  FILE_SYSTEM_CACHE     IO              LOCK
  MODES                 PAGE            POOL
  PROCESSES             SCS             STATES
  SYSTEM

  Qualifiers:
  /BEGINNING            /BY_NODE        /COMMENT
  /DISPLAY              /ENDING         /FLUSH_INTERVAL
  /INPUT                /INTERVAL       /NODE
  /RECORD               /SUMMARY        /VIEWING_TIME

  Class Name Qualifiers:
  /ALL                  /AVERAGE        /CPU
  /CURRENT              /ITEM           /MAXIMUM
  /MINIMUM              /PERCENT        /TOPBIO
  /TOPCPU               /TOPDIO         /TOPFAULT
```

```
MOUNT device_name[:][,...] [volume_label[,...]] [logical_name[:]]
  Invokes the VAX/VMS Mount Utility to make a disk or tape volume available for
  use.

  Qualifiers:
  /ASSIST               /ACCESSED              /AUTOMATIC
  /BIND                 /BLOCKSIZE             /CACHE
  /CLUSTER              /COMMENT               /CONFIRM
  /COPY                 /DATA_CHECK            /DENSITY
  /EXTENSION            /FOREIGN               /GROUP
  /HDR3                 /INITIALIZE            /LABEL
  /MESSAGE              /MOUNT_VERIFICATION    /OVERRIDE
  /OWNER_UIC            /PROCESSOR             /PROTECTION
  /QUOTA                /REBUILD               /RECORDZIDE
  /SHADOW               /SHARE                 /SYSTEM
  /UNLOAD               /WINDOWS               /WRITE


ON condition THEM dcl_command
  Defines the DCL command to be executed when a command or program executed
  with a command procedure encounters an error condition or is interrupted by
  the user pressing <Ctrl-Y>.


OPEN logical_name[:] file_spec
  Opens a file for input/output.  The OPEN command assigns a logical name to
  the file and places the name in the process logical name table.

  Qualifiers:
  /APPEND       /ERROR       /READ       /SHARE       /WRITE


PATCH file_spec
  Invokes the VAX/VMS Patch Utility to patch an executable image, shareable
  image or device driver image.

  Qualifiers:
  /ABSOLUTE     /JOURNAL      /NEW_VERSION      /OUTPUT     /UPDATE
  /VOLUME


PHONE [phone_command]
  Invokes the VAX/VMS Phone Utility.  PHONE provides the facility for you to
  communicate with other users on the system or for any other VAX/VMS system
  connected to your system via a DECnet network.

  Qualifiers:
  /SCROLL       /SWITCH_HOOK      /VIEWPORT_SIZE


PRINT file_spec[,...]
  Queues-up one or more files for printing.

  Qualifiers:
  /AFTER        /BACKUP                /BEFORE         /BURST
  /BY_OWNER     /CHARACTERISTICS       /CONFIRM        /COPIES
  /CREATED      /DELETE                /DEVICE         /EXCLUDE
  /EXPIRED      /FEED                  /FLAG           /FORM
  /HEADER       /HOLD                  /IDENTIFY       /JOB_COUNT
  /LOWERCASE    /MODIFIED              /NAME           /NOTE
  /NOTIFY       /OPERATOR              /PAGES          /PARAMETERS
  /PASSALL      /PRIORITY              /QUEUE          /REMOTE
  /RESTART      /SETUP                 /SINCE          /SPACE
  /TRAILER      /USER


PURGE [file_spec[,...]]
  Deletes all but the highest versions of the specified files.
```

```
  Qualifiers:
  /BACKUP       /BEFORE        /BY_OWNER       /CONFIRM       /CREATED
  /ERASE        /EXCLUDE       /EXPIRED        /KEEP          /LOG
  /MODIFIED     /SINCE


READ logical_name[:] symbol_name
  The READ command inputs a single record from the specified input file and
  assigns the contents of the record to the specified symbol name.

  Qualifiers:
  /DELETE       /END_OF_FILE      /ERROR        /INDEX       /KEY
  /MATCH        /NOLOCK           /PROMPT       /TIME_OUT


RECALL [command_specifier]
  Recalls previously entered commands for reprocessing or correcting.

  Qualifier:
  /ALL


RENAME input_file_spec[,...] output_file_spec
  Modifies the file specification of an existing disk file or disk directory.

  Qualifiers:
  /BACKUP       /BEFORE       /BY_OWNER      /CONFIRM       /CREATED
  /EXCLUDE      /EXPIRED      /LOG           /MODIFIED      /NEW_VERSION
  /SINCE


REPLY ["message"]
  Allows a system operator to communicate with system users.

  Qualifiers:
  /ABORT        /ALL            /BELL                /BLANK_TAPE
  /DISABLE      /ENABLE         /INITIALIZE_TAPE     /LOG
  /NODE         /NOTIFY         /PENDING             /SHUTDOWN
  /STATUS       /TEMPORARY      /TERMINAL            /TO
  /URGENT       /USERNAME       /WAIT


REQUEST "message"
  Writes a message on the system operator's terminal, and optionally requests a
  reply.

  Qualifiers:
  /REPLY        /TO


RETURN [status_code]
  Terminates a GOSUB statement and returns control to the command following the
  GOSUB command.


RUN
  Performs the following functions:
  o  Places an image into execution in the process.
  o  Creates a subprocess or detached process to run a specified image.


RUNOFF
  Performs the following functions:
  o  Invokes the DIGITAL Standard Runoff text formatter to format one or more
     ASCII files.
  o  Invokes the DIGITAL Standard Runoff text formatter to generate a table of
     contents for one or more ASCII files.
  o  Invokes the DIGITAL Standard Runoff text formatter to generate an index
     for one or more ASCII files.
```

```
SEARCH file_spec[,...] search_string[,...]
  Searches one or more files for the specified string(s) and lists all the
  lines containing occurrences of the strings.

  Qualifiers:
  /EXACT        /EXCLUDE        /FORMAT       /HEADING        /LOG
  /MATCH        /NUMBERS        /OUTPUT       /REMAINING      /STATISTICS
  /WINDOW


SET ACCOUNTING
  Enables or disables logging various accounting activities in the system
  accounting log file SYS$MANAGER:ACCOUNTING.DAT.  The SET ACCOUNTING command
  is also used to close the current accounting log file and to open a new one
  with a higher version number.

  Qualifiers:
  /DISABLE      /ENABLE       /NEW_FILE


SET ACL object_name
  Allows you to modify the ACL (access control list) of a VMS object.

  Qualifiers:
  /ACL          /AFTER          /BEFORE         /BY_OWNER       /CONFIRM
  /CREATED      /DEFAULT        /DELETE         /EDIT           /EXCLUDE
  /JOURNAL      /KEEP           /LIKE           /LOG            /MODE
  /NEW          /OBJECT_TYPE    /RECOVER        /REPLACE        /SINCE

SET AUDIT
  Enables or disables VAX/VMS security auditing.

  Qualifiers:
  /ALARM        /DISABLE        /ENABLE


SET BROADCAST = (class_name[,...])
  Allows you to block out various terminal messages from being broadcast to
  your terminal.


SET COMMAND [file_spec[,...]]
  Invokes the VAX/VMS Command Definition Utility to add, delete or replace
  commands in your process command table or a specified command table file.

  Qualifiers:
  /DELETE       /LISTING        /OBJECT         /OUTPUT         /REPLACE
  /TABLE


SET [NO]CONTROL[=(T,Y)]
  Defines whether or not control will pass to the command language interpreter
  when <Ctrl-Y> is pressed and whether process statistics will be displayed
  when <Ctrl-T> is pressed.


SET DAY
  Used to reset the default day type specified in the user authorization file
  for the current day.

  Qualifiers:
  /DEFAULT      /LOG            /PRIMARY        /SECONDARY


SET DEFAULT device_name:directory_spec
  Changes the default device and/or directory specification.  The new default
  is used with all subsequent file operations that do not explicitly include a
  device or directory name.
```

```
SET DEVICE device_name[:]
  Establishes a printer or terminal as a spooled device, or sets the error
  logging status of a device.

  Qualifiers:
  /AVAILABLE    /DUAL_PORT      /ERROR_LOGGING     /LOG
  /SPOOLED


SET DIRECTORY directory_spec[,...]
  Modifies directory characteristics.

  Qualifiers:
  /BACKUP       /BEFORE         /BY_OWNER       /CONFIRM
  /CREATED      /EXCLUDE        /EXPIRED        /LOG
  /MODIFIED     /OWNER_UIC      /SINCE          /VERSION_LIMIT


SET FILE file_spec[,...]
  Modifies file characteristics.

  Qualifiers:
  /BACKUP               /BEFORE         /BY_OWNER           /CONFIRM
  /CREATED              /DATA_CHECK     /END_OF_FILE        /ENTER
  /ERASE_ON_DELETE      /EXCLUDE        /EXPIRATION_DATE    /EXTENSION
  /GLOBAL_BUFFER        /LOG            /NODIRECTORY        /OWNER_UIC
  /PROTECTION           /REMOVE         /SINCE              /UNLOCK
  /TRUNCATE             /VERSION_LIMIT


SET HOST node_name
  Connects your terminal, via your host processor, to another processor in a
  DECnet network.

  Qualifiers:
  /LOG          /DTE          /HSC


SET KEY
  Changes the current key definition state.  Keys are defined by the DEFINE/KEY
  command.

  Qualifiers:
  /LOG          /STATE


SET LOGINS
  Defines the number of users who may gain access to the system.  This command
  also displays the current interactive level.

  Qualifiers:
  /INTERACTIVE


SET MAGTAPE device_name[:]
  Defines default characteristics to be associated with a magnetic tape device
  for subsequent file operations.

  Qualifiers:
  /DENSITY      /END_OF_FILE       /LOG       /LOGSOFT        /REWIND
  /SKIP         /UNLOAD


SET MESSAGE [file_spec]
  Allows you to specify the format of messages, or to override or supplement
  system messages.

  Qualifiers:
  /DELETE      /FACILITY      /IDENTIFICATION       /SEVERITY      /TEXT
```

```
SET [NO]ON
  Controls command interpreter error checking.  If SET NOON is in effect, the
  command interpreter will ignore errors in a command procedure and continue
  processing.


SET OUTPUT_RATE [=delta_time]
  Defines the rate at which output will be written to a batch job log file.


SET PASSWORD
  Permits to change password in a VAX/VMS account

  Qualifiers:
  /GENERATE     /SECONDARY      /SYSTEM


SET PRINTER printer_name[:]
  Defines characteristics for a line printer.

  Qualifiers:
  /CR           /FALLBACK     /FF           /LA11         /LA180
  /LOWERCASE    /LOG          /LP11         /PAGE         /PASSALL
  /PRINTALL     /TAB          /TRUNCATE     /UNKNOWN      /UPPERCASE
  /WIDTH        /WRAP


SET PROCESS [process_name]
  Modifies execution characteristics associated with the named process for the
  current login session.  If a process is not specified, changes are made to
  the current process.

  Qualifiers:
  /CPU          /DUMP           /IDENTIFICATION         /NAME
  /PRIORITY     /PRIVILEGES     /RESOURCE_WAIT          /RESUME
  /SUSPEND      /SWAPPING


SET PROMPT [=string]
  Defines a new DCL prompt for your process.  The default prompt is a dollar
  sign ($).

  Qualifier:
  /CARRIAGE_CONTROL


SET PROTECTION [=(code)] file_spec[,...]
  Modifies the protection applied to a particular file or to a group of files.
  The protection of a file limits the access available to various groups of
  system users.  When used without a file specification, it establishes the
  default protection for all the files subsequently created during the login
  session.  May also be used to modify the protection of a non-file-oriented
  device.

  Qualifiers:
  /CONFIRM      /LOG    /PROTECTION     /DEFAULT      /DEVICE


SET QUEUE queue_name
  Used to modify the current status or attributes of a queue, or to change the
  current status or attributes of a job that is not currently executing in a
  queue.

  Qualifiers:
  /BASE_PRIOTITY     /BLOCK_LIMIT    /CHARACTERISTICS     /CPUDEFAULT
  /CPUMAXIMUM        /DEFAULT        /DISABLE_SWAPPING    /ENABLE_GENERIC
  /FORM_MOUNTED      /JOB_LIMIT      /OWNER_UIC           /PROTECTION
  /RECORD_BLOCKING   /RETAIN         /SCHEDULE            /SEPARATE
```

/WSDEFAULT /WSEXTENT /WSQUOTA /ENTRY

SET RESTART_VALUE=string
Defines a test value for restarting portions of a batch job after a system failure.

SET RIGHTS_LIST id_name[,...]
Allows you to modify the process or system rights list.

Qualifiers:
/ATTRIBUTES /DISABLE /ENABLE /IDENTIFICATION /PROCESS
/SYSTEM

SET RMS_DEFAULT
Used to set default values for the multiblock and multibuffer counts, network transfer sizes, prologue level and extend quantity used by RMS for various file operations.

Qualifiers:

/BLOCK_COUNT	/BUFFER_COUNT	/DISK
/EXTEND_QUANTITY	/INDEXED	/MAGTAPE
/NETWORK_BLOCK_COUNT	/PROLOG	/RELATIVE
/SEQUENTIAL	/SYSTEM	/UNIT_RECORD

SET SYMBOL
Controls access to local and global symbols within command procedures.

Qualifier:
/SCOPE

SET TERMINAL [device_name[:]]
Modifies interpretation of various terminal characteristics.

Qualifiers:

/ADVANCED_VIDEO	/ALTYPEAHD	/ANSI_CRT
/APPLICATION_KEYPAD	/AUTOBAUD	/BLOCK_MODE
/BRDCSTMBX	/BROADCAST	/CRFILL
/DEC_CRT	/DEVICE_TYPE	/DIALUP
/DISCONNECT	/DISMISS	/DMA
/ECHO	/EDIT_MODE	/EIGHT_BIT
/ESCAPE	/FALLBACK	/FRAME
/FORM	/FULLDUP	/HALFDUP
/HANGUP	/HARDCOPY	/HOSTSYNC
/INQUIRE	/INSERT	/LFFILL
/LINE_EDITING	/LOCAL_ECHO	/LOWERCASE
/MANUAL	/MODEM	/NUMERIC_KEYPAD
/OVERSTRIKE	/PAGE	/PARITY
/PASTHRU	/PERMANENT	/PRINTER_PORT
/PROTOCOL	/READSYNC	/REGIS
/SCOPE	/SET_SPEED	/SECURE_SERVER
/SIXEL_GRAPHICS	/SOFT_CHARACTERS	/SPEED
/SWITCH	/SYSPASSWORD	/TAB
/TTSYNC	/TYPE_AHEAD	/UNKNOWN
/UPPERCASE	/WIDTH	/WRAP

SET TIME [=time]
Resets the system time to be used with all time-dependent activities in the VAX/VMS operating system.

SET UIC uic
Establishes a new default user identification code (UIC).

```
SET [NO]VERIFY [=([NO]PROCEDURE,[NO]IMAGE)]
  Controls whether command and data lines, in a command procedure, are
  displayed as they are processed.


SET VOLUME device_spec[:][,...]
  Modifies the characteristics of a mounted Files-11 volume.

  Qualifiers:
  /ACCESSED          /DATA_CHECK             /ERASE_ON_DELETE
  /EXTENSION         /FILE_PROTECTION        /HIGHWATER_MARKING
  /LABEL             /LOG                    /MOUNT_VERIFICATION
  /OWNER_UIC         /PROTECTION             /REBUILD
  /RETENTION         /UNLOAD                 /USER_NAME
  /WINDOWS


SET WORKING_SET
  Sets the default working set size for the current process, or sets an upper
  limit to which the working set size can be changed by an image that the
  process executes.

  Qualifiers:
  /ADJUST      /EXTENT       /LIMIT       /LOG      /QUOTA


SHOW ACCOUNTING
  Displays items for which accounting is enabled.

  Qualifier:
  /OUTPUT


SHOW ACL
  Permits you to display the access control list (ACL) of a VAX/VMS object.

  Qualifier:
  /OBJECT_TYPE


SHOW AUDIT
  Supplies a display that identifies enable security auditing features and the
  events that they will report.

  Qualifier:
  /OUTPUT


SHOW BROADCAST
  Displays messages classes that currently are being affected by the SET
  BROADCAST command.

  Qualifier:
  /OUTPUT


SHOW DEFAULT
  Displays the current default device and directory specification, along with
  any equivalence strings that have been defined.


SHOW DEVICES [device_name[:]]
  Displays the status of a device on the running VAX/VMS system.

  Qualifiers:
  /ALLOCATED    /BRIEF      /FILES        /FULL       /MOUNTED
  /OUTPUT       /SYSTEM     /WINDOWS      /SERVED


SHOW ERROR
```

Displays an error count for all devices with an error count greater than 0.

Qualifiers:
/FULL /OUTPUT

SHOW KEY [key_name]
Displays the key definition for the specified key.

Qualifiers:
/ALL /BRIEF /DIRECTORY /FULL /STATE

SHOW LOGICAL [logical_name[:],[...]]
Displays logical names from one or more logical name tables, or displays the equivalence string(s) assigned to the specified logical names(s).

Qualifiers:
/ACCESS_MODE /ALL /DESCENDANTS /FULL
/GROUP /JOB /OUTPUT /PROCESS
/STRUCTURE /SYSTEM /TABLE

SHOE MAGTAPE device_name[:]
Displays the characteristics and status of a specified magnetic tape device.

Qualifier:
/OUTPUT

SHOW MEMORY
Displays availability and use of memory-related resources.

Qualifiers:
/ALL /FILES /FULL /OUTPUT
/PHYSICAL_PAGES /POOL /SLOTS

SHOW NETWORK
Displays node information about the DECnet network of which your host processor is a member.

Qualifier:
/OUTPUT

SHOW PRINTER device_name[:]
Displays characteristics defined for a system printer.

Qualifier:
/OUTPUT

SHOW PROCESS [process_name]
Displays information about a process and any of its subprocesses.

Qualifiers:
/ACCOUNTING /ALL /CONTINUOUS /IDENTIFICATION /MEMORY
/OUTPUT /PRIVILEGES /QUOTAS /SUBPROCESSES

SHOW PROTECTION
Displays the file protection that will be applied to all new files created during the current login session.

SHOW QUEUE [queue_name]
Displays information about queues and the jobs currently in queue.

Qualifiers:

```
  /ALL          /BATCH          /BRIEF          /DEVICE
  /FILES        /FULL           /OUTPUT         /CHARACTERISTICS
  /FORM


SHOW QUOTA
  Displays the disk quota that is currently authorized for a specific user on a
  specific disk.

  Qualifiers:
  /DISK         /USER


SHOW RMS_DEFAULT
  Displays the default multiblock count, multibuffer count, network transfer
  size, prologue level and extend quantity that RMS will use for file
  operations.

  Qualifier:
  /OUTPUT


SHOW STATUS
  Displays status information for the current process.


SHOW SYMBOL [symbol_name]
  Displays the value of a local or global symbol.

  Qualifiers:
  /ALL          /GLOBAL         /LOCAL          /LOG


SHOW SYSTEM
  Displays a list of processes currently running on a system.

  Qualifiers:
  /BATCH        /FULL         /NETWORK      /OUTPUT     /PROCESS
  /SUBPROCESS


SHOW TERMINAL [device_name[:]]
  Displays the characteristics of a specified terminal.

  Qualifiers:
  /OUTPUT       /PERMANENT


SHOW TIME
  Displays the current system date and time.


SHOW TRANSLATION logical_name
  Searches the logical name tables for a specified logical name, then returns
  the first equivalence name of the match found.

  Qualifier:
  /TABLE


SHOW USERS [username]
  Displays a list of all users currently using the system and their terminal
  names, usernames and their process identification codes.

  Qualifier:
  /OUTPUT


SHOW WORKING_SET
  Displays the current working set limit, quota and extent assigned to the
```

current process.

Qualifier:
/OUTPUT

SORT input_file_spec[,...] output_file_spec
Invokes the VAX/VMS Sort Utility to reorder records in a file into a defined sequence.

Qualifiers:

/COLLATING_SEQUENCE	/DUPLICATES	/KEY
/PROCESS	/SPECIFICATION	/STABLE
/STATISTICS	/WORK_FILES	/FORMAT

Output File Qualifiers:

/ALLOCATION	/BUCKET_SIZE	/CONTIGUOUS
/FORMAT	/INDEXED_SEQUENTIAL	/OVERLAY
/RELATIVE	/SEQUENTIAL	

SPAWN [command_string]
Creates a subprocess to the current process.

Qualifiers:

/CARRIAGE CONTROL	/CLI	/INPUT	
/KEYPAD	/LOG	/LOGICAL_NAMES	
/NOTIFY	/OUTPUT	/PROCESS	
/PROMPT	/SYMBOLS	/TABLE	
/WAIT			

START/QUEUE queue_name
Starts or restarts the specified queue.

STOP process_name
Specifies the name of a process to be deleted from the system. If the /IDENTIFICATION qualifier is used, the process name is ignored.

Qualifier:
/IDENTIFICATION

STOP/QUEUE queue_name[:]
Causes the specified queue to pause.

Qualifiers:

/ABORT	/ENTRY	/MANAGER
/NEXT	/REQUEUE	/RESET

SUBMIT file_spec[,...]
Enters a command procedure(s) into a batch queue.

Qualifiers:

/AFTER	/BACKUP	/BEFORE	/BY_OWNER
/CHARACTERISTICS	/CLI	/CONFIRM	/CPUTIME
/CREATED	/DELETE	/EXCLUDE	/EXPIRED
/HOLD	/IDENTIFY	/KEEP	/LOG_FILE
/MODIFIED	/NAME	/NOTIFY	/PARAMETERS
/PRINTER	/PRIORITY	/QUEUE	/REMOTE
/RESTART	/SINCE	/USER	/WSDEFAULT
/WSEXTENT	/WSQUOTA		

SYNCHRONIZE [job_name]
Places the process issuing the command into a wait state until the specified job completes execution.

```
  Qualifiers:
  /ENTRY        /QUEUE


TYPE file_spec[,...]
  Displays the contents of a file or group of files on the current output
  device (normally your terminal screen).

  Qualifiers:
  /BACKUP       /BEFORE        /BY_OWNER       /CONFIRM       /CREATED
  /EXCLUDE      /EXPIRED       /MODIFIED       /OUTPUT        /PAGE
  /SINCE


UNLOCK file_spec[,...]
  Makes a file that has been made inaccessible as a result of being improperly
  closed accessible.

  Qualifiers:
  /CONFIRM      /LOG


WAIT delta_time
  Places the current process in a wait state until a specified period of time
  has passed.


WRITE logical_name expression[,...]
  Writes the specified data record to the output file indicated by the logical
  name.

  Qualifiers:
  /ERROR        /SYMBOL         /UPDATE


                <:=- Part E : Lexical Function Reference -=:>


 Introduction
 ~~~~~~~~~~~~
Part F is a Lexical Function Reference.  Parameters for the lexicals are in
parenthesis after the function name, and parenthesis are required whether or
not the lexical function requires parameters.


 Lexical Function Reference
 ~~~~~~~~~~~~~~~~~~~~~~~~~~
F$CVSI (bit_position, width, string)
  Used to extract bit fields from a character string.  The result is converted
  to a signed integer value.


F$CFTIME (input_time, output_time, field)
  Converts absolute or combination time to the format yyyy-mm-dd
  hh:mmm:ss.cc.  This function can also be used to return information about an
  absolute, combination, or delta time string.


F$CVUI (bit_position, width, string)
  Extracts bit fields from a character string and converts the result to an
  unsigned integer value.


F$DIRECTORY ()
  Returns the default directory name as a character string.


F$EDIT (string, edit_list)
  Used to edit a character string based on the parameters specified in the
  edit_list.
```

F$ELEMENT (element_number, delimiter, string)
  Extracts an element from a character string in which the elements are
  separated by some specified delimiter.

F$ENVIRONMENT (item)
  Returns information about the DCL command environment.

F$EXTRACT (offset, length, string)
  Extracts a substring from a given character string.

F$FAO (control_string[,arg1,art2...arg15])
  Calls the $FAO system service to convert a specified control string to
  formatted ASCII. This function may be used to insert variable character
  string data into an output string or convert integer values to ASCII and
  substitute the result into the output string.

F$FILE_ATTRIBUTES (file_spec, item)
  Returns attribute information for the specified file.

F$GETDVI (device, item)
  Calls the $GETDVI system service to return an item of information on a
  specified device. This function allows a process to obtain information for a
  device to which the process has not necessarily allocated or assigned a
  channel.

F$GETJPI (pid, item)
  Calls the $GETJPI system service to return status and identification
  information about the running system or about a node in the VAXcluster (if
  the system is a VAXcluster).

F$IDENTIFIER (identifier, conversion_type)
  Converts an identifier into its integer equivalent, or vice versa. An
  identifier is a name or number that identifies a category of data resource
  users. The system uses identifiers to determine user access to a system
  resource.

F$INTEGER (expression)
  Returns the integer value of the result of the specified expression.

F$LENGTH (string)
  Returns the length of a specified character string.

F$LOCATE (substring, string)
  Locates a character or character substring within a string and returns its
  offset within the string. If the character or character substring is not
  found, the function returns the length of the string that was searched.

F$MESSAGE (status_code)
  Returns a character string containing the message associated with a system
  status code.

F$MODE ()
  Returns a character string displaying the mode in which a process is
  executing.

F$PARSE (file_spec[,related_spec][,field][,parse_type])
  Calls the $PARSE RMS service to parse a file specification and return either its expanded file specification or a particular file specification field that you have specified.

F$PID (context_symbol)
  Returns a process identification number (PID), and updates the context symbol to point to the current position in the system's process list.

F$PRIVILEGE (priv_states)
  Returns a value of true or false depending on whether your current process privileges match the privileges listed in the parameter argument.

F$PROCESS ()
  Obtains the current process name as a character string.

F$SEARCH (file_spec[,stream_id])
  Calls the $SEARCH RMS service to search a directory and return the full file specification for a specified file.

F$SETPRV (priv_states)
  Returns a list of keywords indicating current user privileges. In addition, this function may be used to call the $SETPRV system service to enable or disable specified user privileges. The return string indicates the status of the user privileges before any changes have been made with the F$SETPRV function.

F$STRING (expression)
  Returns the character string equivalent of the result of the specified expression.

F$TIME ()
  Returns the current date and time string.

F$TRNLNM (logical_name[,table][,index][,mode][,case][,item])
  Translates a logical name to its equivalence string, or returns the requested attributes of the logical name. The equivalence string is not checked to determine if it is a logical name or not.

F$TYPE (symbol_name)
  Returns the data type of a symbol.

F$USER ()
  Returns the user identification code (UIC), in named format, for the current user. The F$USER function has no arguments.

F$VERIFY ([procedure_value][,image_value])
  Returns an integer value which indicates whether procedure verification mode is currently on or off. If used with arguments, the F$VERIFY function can turn verification mode on or off. You must include the parentheses after the F$VERIFY function, whether or not you specify arguments.

Default File Types

These file types are conventions set by DEC and may not be followed by other software companies.

Type	Contents

Code	Description
ANL	Output file from the ANALYZE command
BAS	Source input file for BASIC compiler
CLD	Command line interpreter command description file
COM	Command procedure file
DAT	Data file (input or output)
DIF	Output file from the DIFFERENCES command
DIR	Subdirectory
DIS	MAIL distribution list
DMP	Output from the DUMP command
EDT	EDT editor initialization file
EXE	VAX/VMS executable program created with the LINK command
FDL	File Definition language file created with the EDIT/FDL or ANALYZE/RMS/FDL command
FOR	Source input for FORTRAN compiler
HLB	Help text library
HLP	Help text file, usually as source input to help text library file
JNL	EDT editor journal file
LIS	List file created by an assembler or compiler
LOG	Information file created by a batch job, DECnet, etc.
MAI	Mail message storage file
MAR	Source input file for MACRO assembler
MLB	MAXCRO source library
OBJ	Intermediate object file created by a compiler or assembler
OLB	Object module library
OPT	Option input file for the LINK command
STB	Symbol table
SYS	System image
TJL	Journal file created by the TPU editor
TLB	Text library
TMP	General purpose temporary file
TPU	Command input file for the TPU editor
TXT	Text file

Device Names
~~~~~~~~~~~~

The following are common VAX/VMS device codes and their corresponding types.

Code	Device Type
CS	Console boot/storage device
DA	RC25 (25 MB fixed/25 MB removable)
DB	RP05, RP06 disk
DD	TU58 tape
DJ	RA60 disk
DL	RL02 disk
DR	RM03 RM05, RM80, RP07 disk
DU	RA80, RA81, RA82 disk
DX	RX01 floppy
DY	RX02 floppy
LC	Line printer device on DMF32
LP	Line printer device on LP11
LT	Local area terminal (LAT)
MB	Mailbox device
MF	TU78 magnetic tape drive
MS	TS11 magnetic tape drive
MT	TU45, TU77, TE16 magnetic tape drive
MU	TK50, TA78, TA81, TU81 magnetic tape drive
NL	Null device
OP	Operators console device
RT	Remote terminal (via DECnet)
TT	Interactive terminal device
TX	Interactive terminal device
VT	Virtual terminal
XE	DEUNA
XQ	DEQNA
~~~~~~~~~~~~

==Phrack Inc.==

Volume Four, Issue Thirty-Eight, File 8 of 15

Wide Area Information Servers

How Do I Use It and Why Should I Care?

by Mycroft
mycroft@gnu.ai.mit.edu

Introduction

This file serves as an introduction to "information servers," and in particular to the WAIS system from Thinking Machines Corp.

Overview

The Wide Area Information Server (or WAIS) system provides a way for people ("providers") to make information sources ("sources") accessible via a network, with a very simple interface to search for and retrieve particular pieces of information ("documents").

Essentially, you pick a source and specify a few keywords, and the WAIS search engine tries to find documents that match those specific keywords. Each document is scored, and the highest scoring documents are listed first. In addition, there is a mechanism ("relevance feedback") for feeding information back to the server about which documents are most interesting to you, and having it narrow the search based on this.

To summarize: WAIS gives you a fast and easy way to search vast amounts of information, and to provide access to it to other users on a network.

Why Should I Care?

You should care because I, through the goodness of my heart, have made all the issues of Phrack Inc. available through WAIS. :-) I'll soon be adding issues of the LOD/H TJ, NARC, NIA, Worldview, and a lot of other files. If anyone would care to donate files, I'd appreciate it.

There are also many other sources currently available that will probably be of interest to you.

Step 1: Compiling A Client

To use WAIS, you need a client program. There are currently 4 available that I know of:

Xwais - for the X Window System
SWAIS - terminal-based
Mac WAIStation
NeXT WAIStation
(I vaguely recall something about a Windows client.)

Xwais and SWAIS both come in the standard distribution, with the search and index engines.

You can FTP any of the above from think.com, in directory /wais. The relevant files are:

wais-8-b4.tar.Z - contains the search and index engines, as well Xwais and SWAIS
WAIStation-0-63.sit.hqx - the Mac WAIStation
WAIStation-NeXT-1.0.tar.Z - the NeXT WAIStation

After you choose a client and get the source, compile it. There are

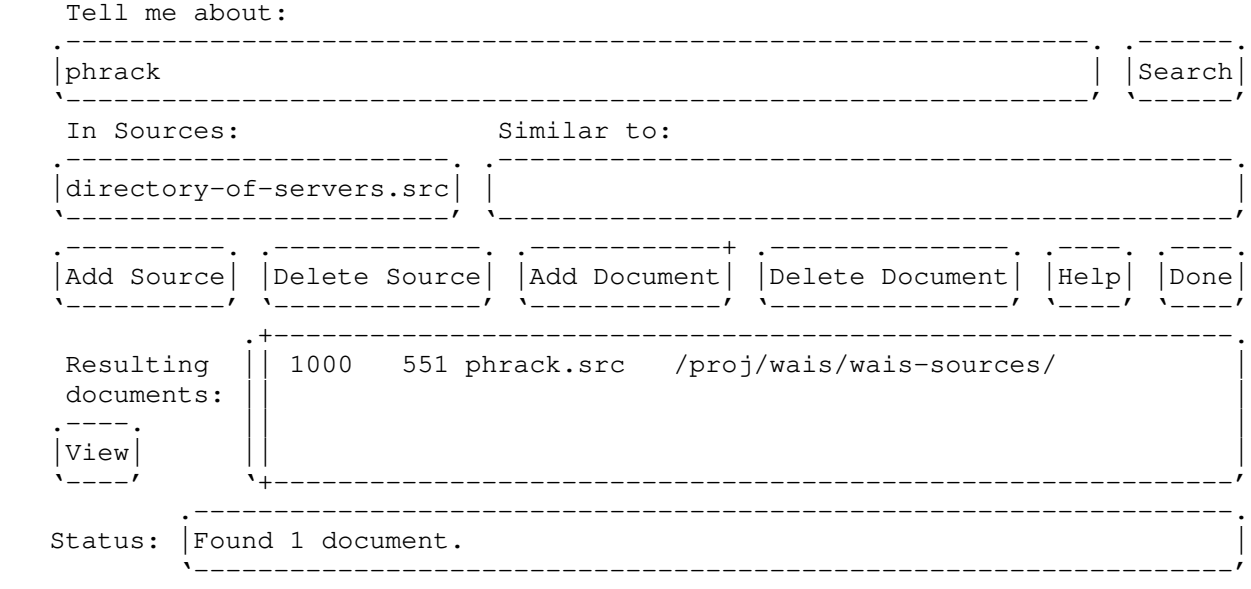
decent directions on how to do this in each package.

Step 2: Finding An Information Source

To find a source, you just do a search in the "directory of servers" -- a source containing pointers to all the registered WAIS sources on the net.

For example, if you're using Xwais:

(I am *not* going to go into the details of how to use the scrollbars and whatnot. If you're stuck, ask a Mac weenie for help.)

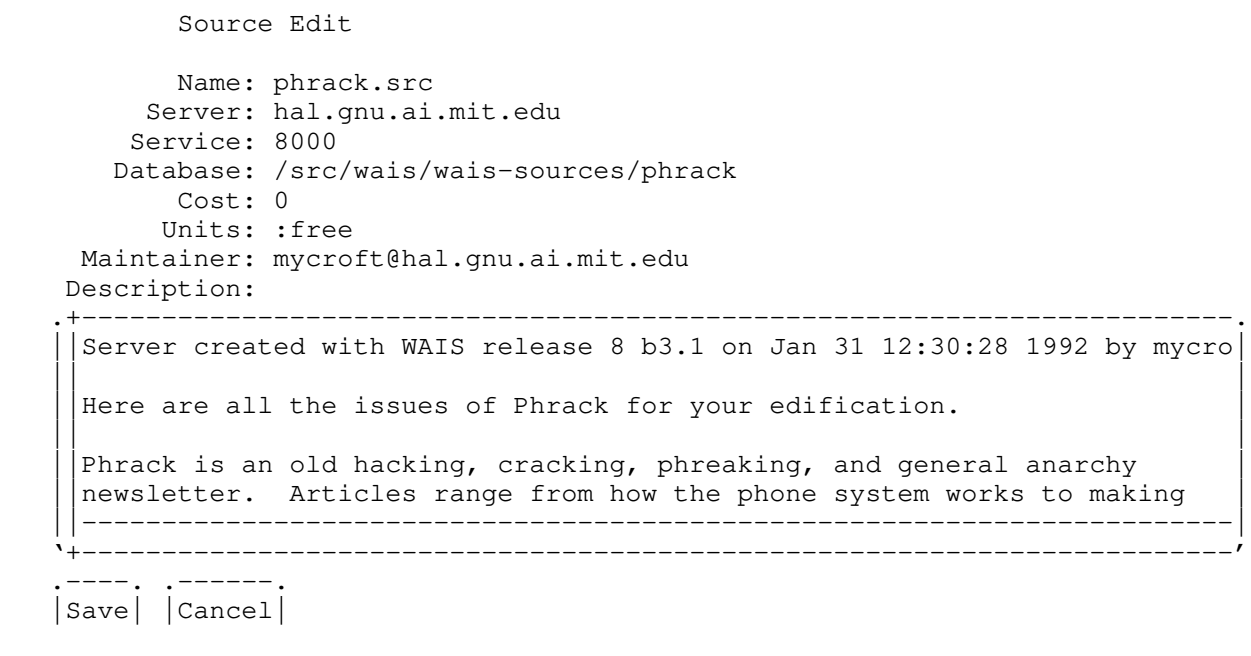


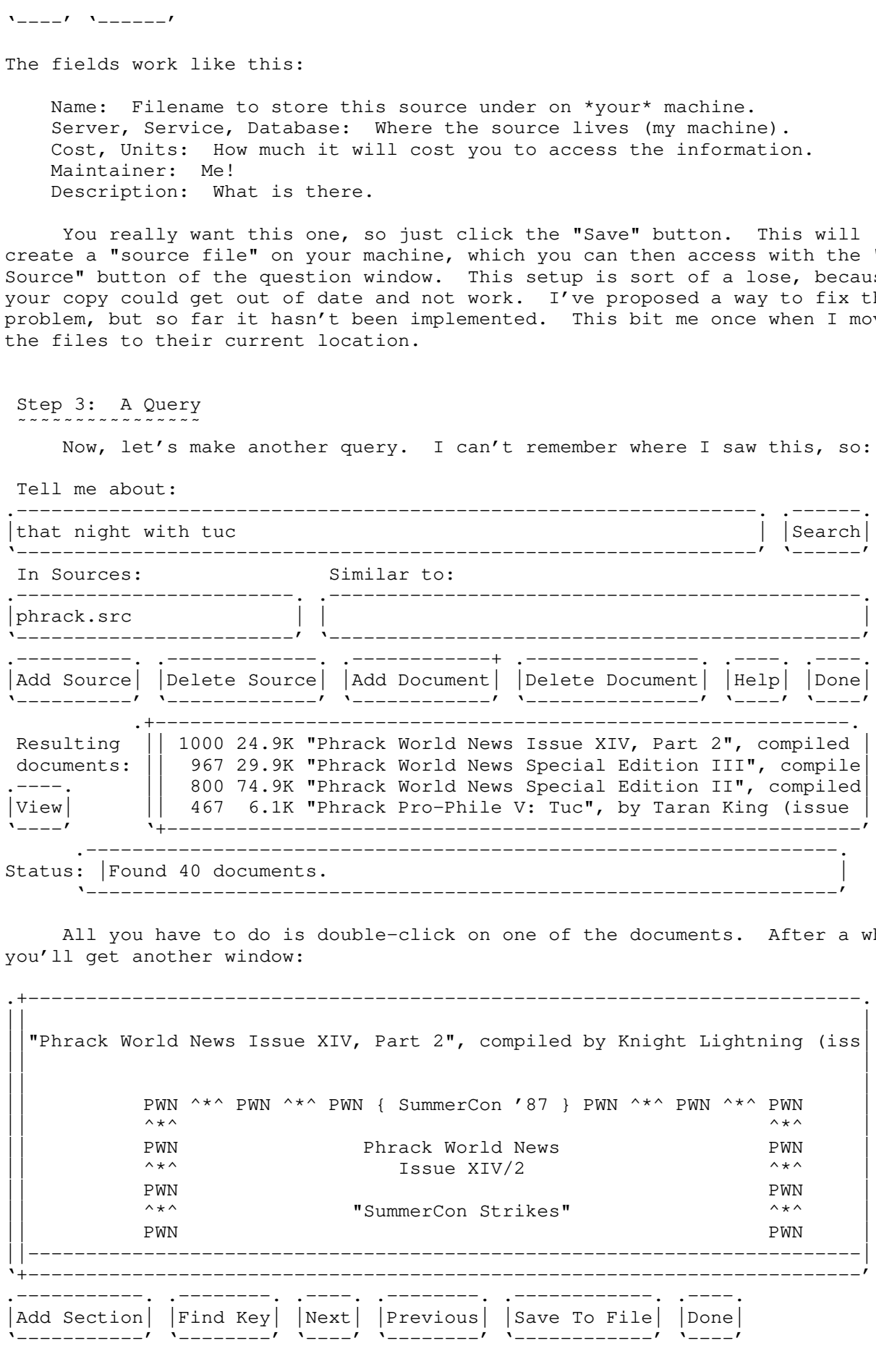
The lines in the "Resulting documents:" window break down into three parts:

```
Score    -- How well it matched your query, as compared to other
            documents.
Size     -- <In bytes> of the document.
Headline -- The "headline" is generated while building the index.
```

For source files, it's broken down by filename and path. For the p/h/c/a server, it's the title of the article, the authors, and the issue and file number.

So double-click on the document, and you'll get another window (shortened a bit):





All you have to do is double-click on one of the documents. After a while you'll get another window:

Status:

The "Add Section" button is used for relevance feedback. You select a region of text and press "Add Section" and it will show up in the "Similar to:" box in the question window.

"Find Key," "Next," and "Previous" are used to search for the keywords in the document. The rest is pretty obvious.

What Else?

There are more powerful ways to use WAIS. For example, using the "waisq" and "waisretrieve" programs, you could query the directory of servers nightly to get the latest copy of phrack.src. This would ensure that yours is never more than a day out of date. (I recommend subscribing to the wais-discussion list and/or reading alt.wais instead, though, since it's more interesting and won't put a load on the directory of servers.)

Or if you keep an archive of your mail, you could use it to index that. (I know several people who do this, including Brewster.)

Or whatever. Take a look at some of the existing sources to get an idea.

Conclusion

WAIS is a very useful tool for finding information. It is still under development, though, and there a few rough edges that need to be worked out. In particular:

* Source files getting out of date.
* Multiple servers for a single source (for reliability and speed).
* Multiple indices for the same source on a given server (for transient information).
* Index overhead. (The Phrack index, for example, is currently larger than the text itself!)

==Phrack Inc.==

Volume Four, Issue Thirty-Eight, File 9 of 15

Cellular Telephony

by

Brian Oblivion

Courtesy of: Restricted-Data-Transmissions (RDT)

"Truth Is Cheap, But Information Costs."

The benefit of a mobile transceiver has been the wish of experimenters since the late 1800's. To have the ability to be reached by another man despite location, altitude, or depth has had high priority in communication technology throughout its history. Only until the late 1970's has this been available to the general public. That is when Bell Telephone (the late Ma Bell) introduced the Advanced Mobile Phone Service, AMPS for short.

Cellular phones today are used for a multitude of different jobs. They are used in just plain jibber-jabber, data transfer (I will go into this mode of cellular telephony in depth later), corporate deals, surveillance, emergencies, and countless other applications. The advantages of cellular telephony to the user/phreaker are obvious:

1. Difficulty of tracking the location of a transceiver (especially if the transceiver is on the move) makes it very difficult to locate.

2. Range of the unit within settled areas.

3. Scrambling techniques are feasible and can be made to provide moderate security for most transmissions.

4. The unit, with modification can be used as a bug, being called upon by the controlling party from anywhere on the globe.

5. With the right knowledge, one can modify the cellular in both hardware and software to create a rather diversified machine that will scan, store and randomly change.

6. ESN's per call thereby making detection almost impossible.

I feel it will be of great importance for readers to understand the background of the Cellular phone system, mainly due to the fact that much of the pioneering systems are still in use today. The first use of a mobile radio came about in 1921 by the Detroit police department. This system operated at 2MHz. In 1940, frequencies between 30 and 40MHz were made available too and soon became overcrowded. The trend of overcrowding continues today.

In 1946, the FCC declared a "public correspondence system" called, or rather classified as "Domestic Public Land Mobile Radio Service" (DPLMRS) at 35 - 44 MHz band that ran along the highway between New York and Boston. Now the 35-44MHz band is used mainly by Amateur radio hobbyists due to the bands susceptibility to skip-propagation.

These early mobile radio systems were all PTT (push-to-talk) systems that did not enjoy today's duplex conversations. The first real mobile "phone" system was the "Improved Mobile Telephone Service" or the IMTS for short, in 1969. This system covered the spectrum from 150 - 450MHz, sported automatic channel selection for each call, eliminated PTT, and allowed the customer to do their own dialing. From 1969 to 1979 this was the mobile telephone service that served the public and business community, and it is still used today.

IMTS frequencies used (MHz):

Channel	Base Frequency	Mobile Frequency
VHF Low Band		
ZO	35.26	43.26
ZF	35.30	43.30
ZH	35.34	43.34
ZA	35.42	43.32
ZY	34.46	43.46
ZC	35.50	43.50
ZB	35.54	43.54
ZW	35.62	43.62
ZL	35.66	43.66
VHF High Band		
JL	152.51	157.77
YL	152.54	157.80
JP	152.57	157.83
YP	152.60	157.86
YJ	152.63	157.89
YK	152.66	157.92
JS	152.69	157.95
YS	152.72	157.98
YA	152.75	158.01
JK	152.78	158.04
JA	152.81	158.07
UHF Band		
QC	454.375	459.375
QJ	454.40	459.40
QO	454.425	459.425
QA	454.45	459.45
QE	454.475	459.475
QP	454.50	459.50
QK	454.525	459.525
QB	454.55	459.55
QO	454.575	459.575
QA	454.60	459.60
QY	454.625	459.625
QF	454.650	459.650

VHF high frequencies are the most popular frequencies of all the IMTS band. VHF low bands are used primarily in rural areas and those with hilly terrain. UHF bands are primarily used in cities where the VHF bands are overcrowded. Most large cities will find at least one station being used in their area.

ADVANCED MOBILE PHONE SYSTEM

The next step for mobile telephone was made in 1979 by Bell Telephone, again introducing the Advanced Mobile Phone Service. This service is the focus of this document, which has now taken over the mobile telephone industry as the standard. What brought this system to life were the new digital technologies of the 1970's. This being large scale integrated custom circuits and microprocessors. Without these technologies, the system would not have been economically possible.

The basic elements of the cellular concept have to do with frequency reuse and cell splitting.

Frequency re-use refers to the use of radio channels on the same carrier frequency to cover different areas which are separated by a significant distance. Cell splitting is the ability to split any cell into smaller cells if the traffic of that cell requires additional frequencies to handle all the area's calls. These two elements provide the network an opportunity to handle more simultaneous calls, decrease the transmitters/receivers output/input wattage/gain and a more universal signal quality.

When the system was first introduced, it was allocated 40MHz in the frequency spectrum, divided into 666 duplex radio channels providing about 96 channels per cell for the seven cluster frequency reuse pattern. Cell sites (base stations) are located in the cells which make up the cellular network. These cells are usually represented by hexagons on maps or when developing new systems and layouts. The cell sites contain radio, control, voice frequency processing and maintenance equipment, as well as transmitting and receiving antennas. The cell sites are inter-connected by landline with the Mobile Telecommunications Switching Office (MTSO).

In recent years, the FCC has added 156 frequencies to the cellular bandwidth. This provides 832 possible frequencies available to each subscriber per cell. All new cellular telephones are built to accommodate these new frequencies, but old cellular telephones still work on the system. How does a cell site know if the unit is old or new? Let me explain.

The problem of identifying a cellular phones age is done by the STATION CLASS MARK (SCM). This number is 4 bits long and broken down like this:

Bit 1: 0 for 666 channel usage (old)
1 for 832 channel usage (new)

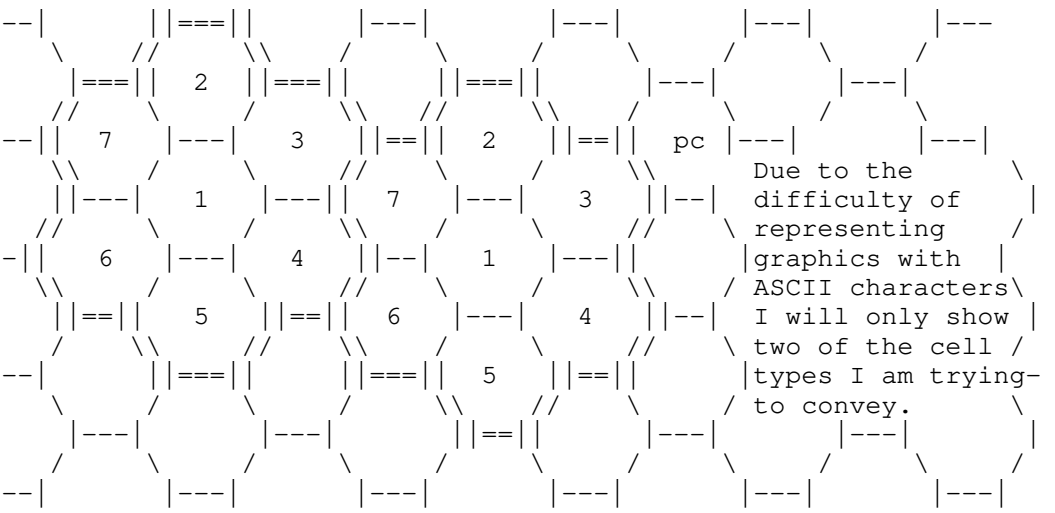
Bit 2: 0 for a mobile unit (in vehicle)
1 for voice-activated transmit (for portables)

Bit 3-4: Identify the power class of the unit

Class I	00 = 3.0 watts Continuous Tx's	00XX...DTX <> 1
Class II	01 = 1.2 watts Discont. Tx's	01XX...DTX = 1
Class III	10 = 0.6 watts reserved	10XX, 11XX
Reserved	11 = ---------	Letters DTX set to 1 permits use of discontinuous trans-missions

Cell Sites: How Cellular Telephones Get Their Name

Cell sites, as mentioned above are laid out in a hexagonal type grid. Each cell is part of a larger cell which is made up of seven cells in the following fashion:



As you can see, each cell is a 1/7th of a larger cell. Where one (1) is the center cell and two (2) is the cell directly above the center. The other cells are number around the center cell in a clockwise fashion, ending with seven (7). The cell sites are equipped with three directional antennas with an RF beamwidth of 120 degrees providing 360 degree coverage for that cell. Note that all cells never share a common border. Cells which are next to each other are obviously never assigned the same frequencies. They will almost always differ by at least 60 KHz. This also demonstrates the idea behind cell splitting. One could imagine that the parameter of one of the large cells was once one cell. Due to a traffic increase, the cell had to be sub-divided to

provide more channels for the subscribers. Note that subdivisions must be made in factors of seven.

There are also Mobile Cell sites, which are usually used in the transitional period during the upscaling of a cell site due to increased traffic. Of course, this is just one of the many uses of this component. Imagine you are building a new complex in a very remote location. You could feasibly install a few mobile cellular cell sites to provide a telephone-like network for workers and executives. The most unique component would be the controller/transceiver which provides the communications line between the cell site and the MTSO. In a remote location such a link could very easily be provided via satellite up/down link facilities.

Let's get into how the phones actually talk with each other. There are several ways and competitors have still not set an agreed upon standard.

Frequency Division Multiple Access (FDMA)

This is the traditional method of traffic handling. FDMA is a single channel per carrier analog method of transmitting signals. There has never been a definite set on the type of modulation to be used. There are no regulations requiring a party to use a single method of modulation. Narrow band FM, single sideband AM, digital, and spread-spectrum techniques have all been considered as a possible standard, but none have yet to be chosen.

FDMA works like this: Cell sites are constantly searching out free channels to start out the next call. As soon as a call finishes, the channel is freed up and put on the list of free channels. Or, as a subscriber moves from one cell to another, the new cell they are in will hopefully have an open channel to receive the current call in progress and carry it through its location. This process is called handoff, and will be discussed more in depth further along.

Other proposed traffic handling schemes include Time-Division Multiple Access (TDMA), Code-Division Multiple Access (CDMA), and Time-Division/Frequency Division Multiple Access (TD/FDMA).

Time Division Multiple Access

With TDMA, calls are simultaneously held on the same channels, but are multiplexed between pauses in the conversation. These pauses occur in the way people talk and think, and the telephone company also injects small delays on top of the conversation to accommodate other traffic on that channel. This increase in the length of the usual pause results in a longer amount of time spent on the call. Longer calls result in higher costs of the calls.

Code Division Multiple Access

This system has been used in mobile military communications for the past 35 years. This system is digital and breaks up the digitized conversation into bundles, compresses, sends, then decompresses and converts back into analog. There are said increases of throughput of 20 : 1 but CDMA is susceptible to interference which will result in packet retransmission and delays. Of course, error correction can help in data integrity, but will also result in a small delay in throughput.

Time-Division/Frequency Division Multiple Access

TD/FDMA is a relatively new system which is an obvious hybrid of FDMA and TDMA. This system is mainly geared towards the increase of digital transmission over the cellular network. TD/FDMA make it possible to transmit signals from base to mobile without disturbing the conversation. With FDMA, there are significant disturbances during handoff which prevent continual data transmission from site to site. TD/FDMA makes it possible to transmit control signals by the same carrier as the data/voice thereby ridding extra channel usage for control.

Cellular Frequency Usage and channel allocation

There are 832 cellular phone channels which are split into two separate bands. Band A consists of 416 channels for non-wireline services. Band B consists equally of 416 channels for wireline services. Each of these channels are split into two frequencies to provide duplex operation. The lower frequency is for the mobile unit while the other is for the cell site. 21 channels of each band are dedicated to "control" channels and the other 395 are voice channels. You will find that the channels are numbered from 1 to 1023, skipping channels 800 to 990.

I found these handy-dandy equations that can be used for calculating frequencies from channels and channels from frequencies.

```
N = Cellular Channel #          F = Cellular Frequency
B = 0 (mobile) or B = 1 (cell site)



CELLULAR FREQUENCIES from CHANNEL NUMBER:


F = 825.030 + B * 45 + ( N + 1 ) * .03
        where:  N = 1 to 799

F = 824.040 + B * 45 + ( N + 1 ) * .03
        where:  N = 991 to 1023



CHANNEL NUMBER from CELLULAR FREQUENCIES


N = 1 + (F - 825.030 - B * 45) / .03

        where:  F >= 825.000 (mobile)
             or F >= 870.030 (cell site)

N = 991 + (F - 824.040 - B * 45) / .03

        where:  F <= 825.000 (mobile)
             or F <= 870.000 (base)
```

Now that you have those frequencies, what can you do with them? Well, for starters, one can very easily monitor the cellular frequencies with most hand/base scanners. Almost all scanners pre-1988 have some coverage of the 800 - 900 MHz band. All scanners can monitor the IMTS frequencies.

Remember that cellular phones operate on a full duplex channel. That means that one frequency is used for transmission and the other is used for receiving, each spaced exactly 30 KHz apart. Remember also that the base frequencies are 45MHz higher than the cellular phone frequencies. This can obviously make listening rather difficult. One way to listen to both parts of the conversation would be having two scanners programmed 45 MHz apart to capture the entire conversation.

The upper UHF frequency spectrum was "appropriated" by the Cellular systems in the late 1970's. Televisions are still made to receive up to channel 83. This means that you can receive much of the cellular system on you UHF receiver. One television channel occupies 6MHz of bandwidth. This was for video, sync, and audio transmission of the channel. A cellular channel only takes up 24 KHz plus 3KHz set up as a guard band for each audio signal. This means that 200 cellular channels can fit into one UHF television channel. If you have an old black and white television, drop a variable cap in there to increase the sensitivity of the tuning. Some of the older sets have coarse and fine tuning knobs.

Some of the newer, smaller, portable television sets are tuned by a variable resistor. This make modifications MUCH easier, for now all you have to do is drop a smaller value pot in there and tweak away. I have successfully done this on two televisions. Most users will find that those who don't live in a

city will have a much better listening rate per call. In the city, the cells are so damn small that handoff is usually every other minute. Resulting in chopped conversations.

If you wanted to really get into it, I would suggest you obtain an old television set with decent tuning controls and remove the RF section out of the set. You don't want all that hi-voltage circuitry lying around (flyback and those caps). UHF receivers in televisions downconvert UHF frequencies to IF (intermediate frequencies) between 41 and 47 MHz. These output IF frequencies can then be run into a scanner set to pick-up between 41 - 47 MHz. Anyone who works with RF knows that it is MUCH easier to work with 40MHz signals than working with 800MHz signals. JUST REMEMBER ONE THING! Isolate the UHF receiver from your scanner by using a coupling capacitor (0.01 - 0.1 microfarad <50V minimum> will do nicely). You don't want any of those biasing voltages creeping into your scanner's receiving AMPLIFIERS! Horrors. Also, don't forget to ground both the scanner and receiver.

Some systems transmit and receive the same cellular transmission on the base frequencies. There you can simply hang out on the base frequency and capture both sides of the conversation. The handoff rate is much higher in high traffic areas leading the listener to hear short or choppy conversations. At times you can listen in for 5 to 10 minutes per call, depending on how fast the caller is moving through the cell site.

TV Channel	Cell & Channel Freq.& Number	Scanner Frequency	TV Oscillator Frequency	Band Limit
73 (first)	0001 - 825.03	45.97	871	824 - 830
73 (last)	0166 - 829.98	41.02	871	824 - 830
74 (first)	0167 - 830.01	46.99	877	830 - 836
74 (last)	0366 - 835.98	41.02	877	830 - 836
75 (first)	0367 - 836.01	46.99	883	836 - 842
75 (last)	0566 - 841.98	41.02	883	836 - 842
76 (first)	0567 - 842.01	46.99	889	842 - 848
76 (last)	0766 - 847.98	41.02	889	842 - 848
77 (first)	0767 - 848.01	46.99	895	848 - 854
77 (last)	0799 - 848.97	46.03	895	848 - 854

All frequencies are in MHz

You can spend hours just listening to cellular telephone conversations, but I would like to mention that it is illegal to do so. Yes, it is illegal to monitor cellular telephone conversations. It just another one of those laws like removing tags off of furniture and pillows. It's illegal, but what the hell for? At any rate, I just want you to understand that doing the following is in violation of the law.

Now back to the good stuff.

Conversation is not only what an avid listener will find on the cellular bands. One will also hear call/channel set-up control data streams, dialing, and other control messages. At times, a cell site will send out a full request for all units in its cell to identify itself. The phone will then respond with the appropriate identification on the corresponding control channel.

Whenever a mobile unit is turned on, even when not placing a call, whenever there is power to the unit, it transmits its phone number and its 8-digit ID number. The same process is done when an idling phone passes from one cell to the other. This process is repeated for as long as there is power to the unit. This allows the MTSO to "track" a mobile through the network. That is why it is not a good reason to use a mobile phone from one site. They do have ways of finding you. And it really is not that hard. Just a bit of RF Triangulation theory and you're found. However, when the power to the unit is shut off, as far as the MTSO cares, you never existed in that cell, of course unless your unit was flagged for some reason. MTSO's are basically just ESS systems designed for mobile applications. This will be explained later within this document.

It isn't feasible for the telephone companies to keep track of each customer on the network. Therefore the MTSO really doesn't know if you are authorized to

use the network or not. When you purchase a cellular phone, the dealer gives the unit's phone ID number to the local BOC, as well as the number the BOC assigned to the customer. When the unit is fired up in a cell site its ID number and phone number are transmitted and checked. If the two numbers are registered under the same subscriber, then the cell site will allow the mobile to send and receive calls. If they don't match, then the cell will not allow the unit to send or receive calls. Hence, the most successful way of reactivating a cellular phone is to obtain an ID that is presently in use and modifying your ROM/PROM/EPROM for your specific phone.

RF and AF Specifications:

Everything that you will see from here on out is specifically Industry/FCC standard. A certain level of compatibility has to be maintained for national intercommunications, therefore a common set of standards that apply to all cellular telephones can be compiled and analyzed.

Transmitter Mobiles: audio transmission

- 3 KHz to 15 KHz and 6.1 KHz to 15 KHz.
- 5.9 KHz to 6.1 KHz 35 dB attenuation.
- Above 15 KHz, the attenuation becomes 28 dB.
- All this is required after the modulation limiter and before the modulation stage.

Transmitters Base Stations: audio transmission

- 3 KHz to 15 KHz.
- Above 15 KHz, attenuation required 28 dB.
- Attenuation after modulation limiter – no notch filter required.

RF attenuation below carrier transmitter: audio transmission

- 20 KHz to 40 KHz, use 26 dB.
- 45 KHz to 2nd harmonic, the specification is 60 dB or 43 + 10 log of mean output power.
- 12 KHz to 20 KHz, attenuation 117 log f/12.
- 20 KHz to 2nd harmonic, there is a choice: 100 log F/100 or 60 dB or 43 log + 10 log of mean output power, whichever is less.

Wideband Data

- 20 KHz to 45 KHz, use 26 dB.
- 45 KHz to 90 KHz, use 45 dB.
- 90 KHz to 2nd harmonic, either 60 dB or 43 + 10 log mean output power.
- all data streams are encoded so that NRZ (non-return-to-zero) binary ones and zeroes are now zero-to-one and one-to-zero transitions respectively. Wideband data can then modulate the transmitter carrier by binary frequency shift keying (BFSK) and ones and zeroes into the modulator must now be equivalent to nominal peak frequency deviations of 8 KHz above and below the carrier frequency.

Supervisory Audio Tones

- Save as RF attenuation measurements.

Signaling Tone

- Same as Wideband Data but must be 10 KHz +/- 1 Hz and produce a nominal frequency deviation of +/- 8 KHz.

The previous information will assist any technophile to modify or even troubleshoot his/her cellular phone. Those are the working guidelines, as I stated previously.

UNIT IDENTIFICATION

Each mobile unit is identified by the following sets of numbers.

The first number is the Mobile Identification Number (MIN). This 34 bit binary number is derived from the unit's telephone number. MIN1 is the last seven digits of the telephone number and MIN2 is the area code.

For demonstrative purposes, we'll encode 617-637-8687.

Here's how to derive the MIN2 from a standard area code. In this example, 617 is the area code. All you have to do is first convert to modulo 10 using the following function. A zero digit would be considered to have a value of 10.

100(first number) + 10(second) +1(third) - 111 = x

100(6) + 10(1) + 1(7) - 111 = 506

(or you could just - 111 from the area code.)

Then convert it to a 10-bit binary number: 0111111010.

To derive MIN1 from the phone number is equally as simple. First encode the next three digits, 637.

100(6) + 10(3) + 1(7) - 111 = 526

Converted to binary: 1000001110

The remainder of the number 8687, is processed further by taking the first digit, eight (8) and converting it directly to binary.

8 = 1000 (binary)

The last three digits are processed as the other two sets of three numbers were processed.

100(6) + 10(8) + 1(7) - 111 = 576

Converted to binary: 1001000000.

So the completed MIN number would look like this:

```
|--637---||8-||---687--||---617--|
10000011101000100100000000111111010
\_________/\__/\_________/\_________/
```

A unit is also identifiable by its Electronic Serial Number or ESN. This number is factory preset and is usually stored in a ROM chip, which is soldered to the board. It may also be found in a "computer on a chip," which are the new microcontrollers which have ROM/RAM/microprocessor all in the same package. This type of set-up usually has the ESN and the software to drive the unit all in the same chip. This makes is significantly harder to dump, modify and replace. But it is far from impossible.

The ESN is a 4 byte hex or 11-digit octal number. I have encountered mostly 11-digit octal numbers on the casing of most cellular phones. The first three digits represent the manufacturer and the remaining eight digits are the unit's ESN.

The Station Class Mark (SCM) is also used for station identification by providing the station type and power output rating. This was already discussed in a previous section.

The System IDentification (SID number is a number which represents the mobile's home system. This number is 15-bits long and a list of current nationwide SID's should either be a part of this file or it will be distributed along with it.
