==Phrack Inc.==

Volume One, Issue Five, Phile #1 of 12

Intro to Phrack V!
~~~~~ ~~ ~~~~~~ ~~
4/18/86

Welcome to Phrack Inc. Issue Five! Thanks to you, the readers, we have received a good following and will continue to pump out issues! Your support has been fantastic and I'm happy to say that more people out there that know their stuff are coming out of the woodwork and writing philes to be distributed with Phrack Inc. Recently, I received a letter from a law firm in New York complaining about the Master Lock Picking phile in Issue One of Phrack Inc. This was written by Ninja NYC and Gin Fizz, both of The Punk Mafia. It was a top class phile and it worked...but that was the problem. They wished me to do something about the material stated. Details of this story can be read in this edition of Phrack World News. Let me state here though, all philes that are distributed with Phrack Inc. are merely being transmitted, and we are not responsible for the philes' content any more than the readers are. The philes are the responsibility of the writers, and I'm not trying to lay the blame on Ninja NYC and Gin Fizz (see the letter I wrote to the firm stating my position here), but we will not be blamed for a crime that has not been committed. Look forward to many more issues of Phrack Inc. in the far future!

TARAN KING
Sysop of Metal Shop Private

This issue contains the following philes:

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

==========
=
~~~~~

==Phrack Inc.==

Volume One, Issue Five, Phile #2 of 12

==Phrack Pro-Phile II==

Written and Created by Taran King

4/5/86

Welcome to Phrack Pro-Phile II. 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 controversial users of our times and
of days of old...

Broadway Hacker

Broadway Hacker is the sysop of The Radio Station, a phreak/hack bulletin board in Brooklyn, N.Y. (718).

Personal

```
            Handle: Broadway Hacker
         Call him: Mike
      Past handles: None (except his sysop handle, "The Program Director")
     Handle origin: Thought it up while on Compu-Serve
     Date of Birth: April 22, 1965
Age at current date: 20 years old
            Height: 6'2"
            Weight: About 150 lbs.
         Eye color: Green/Hazel
        Hair Color: Brown
          Computer: Commodore 64 with 3 disk drives and 300/1200 baud modem
 Sysop/Co-Sysop of: The Radio Station, The Night Stalker
```

Broadway Hacker started out in the BBS world in late 1983 when he first got his modem. On March 23, 1985, The Broadway Show, his first bulletin board, was launched into the BBS world. It started on 1 disk drive at 300 baud
and has upgraded incredibly. It was originally a phreak board as it currently is also. He had originally gotten his C-64 computer in early 1985. Various members of the elite world including King Blotto, Lex Luthor, and Dr. Who got on his board to make it the memorable board that it was before the format change. His phreak experience began in 1981 through CB radios when a CB'er gave him a code over the line. Some of the memorable phreak boards he was on included Blottoland, The AT&T Phone Center of 312, and Dark Side of the Moon of
818. He gives credit for his phreak knowledge to conferences mostly. The Radio

Mike works at a very large radio station. His phreaking is unknown at
work. He's not particularly interested in programming beyond modifying The Radio Station.

Broadway Hacker hasn't the time for hacking now. Broadway attends the

Tap meetings in New York occasionally, but in the past he was a regular. He attended the 1986 TelePub meeting in New York which was to decide the fate of Tap magazine. Broadway has met various phreaks in person including BIOC Agent 003, Lex Luthor, Dr. Who, King Blotto, Cheshire Catalyst, The Sprinter, The Saint, Micro Ghoul, 2600 Magazine People, Paul Muad'Dib, and TUC. There were others, but he couldn't remember at 9:00 AM EST. He has made it a point to not
become a member of groups, but he has been, in the past, invited to many.

Interests: Traveling, radio, telecommunications (modeming, phreaking), trashing, meeting other phreaks, BBS'ing, and running The Radio Station.

Broadway Hacker's Favorite Things

Women: No names mentioned but yes...
Cars: Fieros
Foods: Ray's Pizza (West 11th and 6th Ave.), Steve's Ice Cream
Music: Any top 40 groups in general.

Most Memorable Experiences

Getting almost kidnapped by a gay bellhop in Denver
Getting stranded in California

Some People to Mention

Sigmund Fraud (an up-and-coming phreak who has learned a lot in a short time)

Broadway Hacker wishes you all to know that he does not conference at all any more because conferencing has depreciated from the old days and that they have become mostly a place to gather for gossip.

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? For the most part, Broadway says, "No".
Thanks for your time Mike.

TARAN KING
SYSOP OF METAL SHOP PRIVATE

==Phrack Inc.==

Volume One, Issue Five, Phile #3 of 12

```
[/][/][/][/][/][/][/][/][/][/][/][/][/]
[/] Hacking the Dec-10 system [/]
[/]         written by,       [/]
[/]       Carrier Culprit     [/]
[/][/][/][/][/][/][/][/][/][/][/][/][/]
```
Revised Edition....

Note: This file was distributed by accident, it was not finished. This is the new and revised edition. If you see my file distributed on some AE, BBS, Catfur, and it's not the revised edition please ask the sysop to delete it. Thank-you.

Part I: Logging In, and simple cmds.

Note:Sysop's may download this file
but please keep the appropriate
credits.

Welcome to Hacking Dec 10's!

There is one way to recognize a Dec-10, you will get the "." prompt. First there will be a little login message, sort of like a login on a BBS. For example-

```
NIH Timesharing

NIH Tri-SMP 7.02-FF  19:57:11 TTY12
system 1378/1381/1453 Connected to Node Happy(40) Line # 13
Please LOGIN
.
```

Now, you've gotten so far that you have found a Dec (Digital Equipment Corp), you will need to know the format of the login.

[Login format]

The users have numbers called PPN's which stands for "Project/Program Number".
The format of a PPN number is [X,X]. The first number is the the Project number
and the second is the Program Number.

ie-

```
.Log 12,34

Job 64 NIH 7.01 KL 64-UC TTY12
Password:
```

The password can range from 1-8 characters long, it may contain numbers, initials, or something of the sort. Try and think, if I were a user what would my password be. I doubt that method would work but it's worth a try.

Now say this is your very first time on a Dec 10 system. Now if you want to see some information about the system and some commands you may want to type-

.Help

 This will tell a little more about the system you are on. It will tell you how
to get information on a specific topic. It may also give you the number to their voice dial-up just in case your having trouble.
 Now the dial-up (voice) may help you if your good in BS'ing. Usually the Help command will tell you to consult your 'Dec 10-system guide' for more information.

  Now say you want a list of commands to execute. You can type-
.Help *

 You will then get the following commands- Which are too many to type in but you will recognize them when you type Help *.

 Now after it shows all the commands it will then tell you how to login. It will not give you a demo account, but will give you an example login.

 It will say something like, "The Login command is used for accessing the Decsystem-10 timesharing system."

  To login please enter your project,programmer number pair.

 LOGIN XXX,XXXX

 The system will prompt you for your password. If your PPN or password is wrong you will then be prompted with a message that says-

Enter Project,programmer #xxx,xxxx
Password:

End of that.

 Now, there are some other useful commands you may enter while still *not* having a account. You can access Decnet which I will discuss later which is very nice to a hacker.

 Now, there is also a command you can execute called "Help Phone". What this does is, it lists the numbers of different Dec related staffs. etc....
Example-

.Help Phone

DCRT/CCB/DECsystem-10 Information Phone numbers (4/86)

Recorded message	Dial xxx-xxxx
Dec-10 operator	Dial xxx-xxxx
Dec-10 staff	Dial xxx-xxxx
Terminal Repairs	Dial xxx-xxxx
Classes/Courses	Dial xxx-xxxx
Users Area Phone	Dial xxx-xxxx
Project Control Office	Dial xxx-xxxx

NOTE:This is the same area code as the Decsystem.

 Now the two numbers which would be the most important to you would be the number of the Dec10 operator and the Dec10 staff.

 Now the most important command which can be executed on the Dec10 which is good to use is "Systat"; this will list PPN's, time, running job, time elapsed.

Once you get that PPN you can start hacking away. Using systat is the simplest
and easiest way to get PPN's. It will just be easier to type "SY" instead of "Systat", they are both the same thing except sy is the abbreviation.

Now here's a little example of what you would get by executing the "sy" command.

```
.SY

Status of Brown University 603A at 11:52:33 on 29-Jan-86

Uptime 187:12:22, 80%Null time = 80%idle + 0%Lost
7 Jobs in use out of 128. 19 logged in 4 detached out of 89   (LOGMAX)
Job    Who    What    Run Time

 1    [OPR]   OPSER     3:22
 2    [OPR]   DIALOG    1:29
 3    [OPR]   BATCON    4:01
 4    [OPR]   SYSINF   51:13 01
 5    24,2    SYSTAT    4:52
 6  2332,21   DIRECT    2:22
 7    32,22   SYSTAT    8:19
```

There will also be more stuff along with the above. Now you shouldn't concern yourself with it, that's why I didn't add in. Now also there will be more sub-headings than run time, who, what, and job. You also shouldn't concern yourself with that either.

Now everything is really self explanatory which is up there. Now for beginners who are reading this file I will just tell you what that means Job is
no concern. Who is telling you what kind of person is on the system. [OPR] means Operator, and the numbers such as, 24,2 are referring to regular users with PPN's. Now the next column which is "What". This is telling us what they are executing or what they are presently doing on the system. Run time is telling us what time they logged in. They are using military time. Now under systat you can find: System File Structures, Busy devices, Height segments, and
Disk Structure. Don't worry about that stuff now.

Now you've finally got yourself some PPN's, well the next thing to do is to login using the procedure I showed you with Log. Enter the PPN xx,xx, and try to hack out some passwords.

I will now give you a list of passwords which I have currently used to get into a Dec10. If these passwords don't work well I am sorry you'll just have to
try some yourself.

Note: You can also make a little program having it testing out different PPN's and Passwords.

List of Passwords--

Sex	Dec	Decnet
Games	Test	Dcl
System	Computer	Password
Help	Link	List
Secret	Default	Modem
Account	Terminal	Acsnet

```
Ppn           Operator       Connect
-------------------------------------
```

There are many more passwords people use but I just put some common ones.

You can also try random passwords like, AA, AAB, AB, CC, etc..

Now that is it on logging in. I spent a little too much time on this but since this will be a two part file, I will discuss more commands that I don't get around to discuss in here in part II. Now this file is intended for the beginner so you experienced Dec hackers are bored now or will get bored later.

Note: If connected to Acsnet, just type AcsDec10 to access the Dec. Everything else that I mentioned in the login will work.

[In the system]

Now will assume you've finally gotten into the system after hacking your brains out. Now, this is how you will know you are in the system.
Example-

```
.Login 21,34
Password:
```

Note: You usually get two tries to enter PPN and Password.

The Dec will introduce itself, saying when the last time you were on, etc.

Also if you may do something like this to log-on.

```
.Log 12,34
JOB 51 NIH 7.01 KL 64-UC TT12
Password:[c/r]
Other jobs detached with same PPN:
Job 34 running SYSTAT in ^C state
Do you want to ATTACH to this job? yes


Attaching to job 34
```

Now, what you are doing is attaching to an idle PPN. See, while someone else is on the system, about 10 minutes <max=15 mins> before you, they can input a command that will allow them to logoff and he can attach back to that PPN when he logs back on. That person will then be put to the place where he logged off at. If I were using 'sys', and I logged off. I would use the command 'detach'. Now the person would have 15 minutes to call back and attach to his PPN. There's one other way to attach to an account. If the person doesn't type something for awhile he will automatically be logged off and if you call within
15 minutes you may be able to attach to his PPN.

Note: You may still have to login.

Ok, we are now in the system after it has verified itself. What do we do? Well
first let's take another look at the "systat". We notice there is one other person logged in. But we see he is in "exe", this means he is doing nothing or he's detached. In other words, don't worry about it.
Now if we wanted to change our password, we would type-

```
/Password
```

After we do this, the system will ask us for our old password and our new password, but we should leave the password the way it is so we won't be discovered. But it's a good thing to know.

Now we can take a look at other users files. We can do this by typing-

Dir [*,*]

*=Wildcard

This will show you files of users who have their files set for public access. Now lets say we want to take a look at someone's file. We would type-

Dir [12,11]

If 12,11 was the user number we wanted we would type that inside the brackets.

Now there are many types of files. Now you may have looked through someone's dir, or looked through a wildcard and noticed some files. On most files you may
have seen the words 'txt' or 'exe'.

For exe you will type-

[PPN]filename.exe

for txt you will type-
type filename.txt

You may also see file types such as: dat, bas, cmd, pcl, bin, hlp, and some others.

<1>Exe=executable, which means that you can run these files from the "." prompt.

<2>Txt=Text, these are text files which may contain: information, data or other
numerous things. These are files you may see on most every user who has a public directory, and I find the most popular on Dec-10's.

<3>Bas=Basic, these files are written in of course basic, and must be used in basic. To enter that on a Dec-10, just simply type Run Bas or if that doesn't work type plain old basic.

Note: The basic files are to be used like any other basic file, load them up and run them.

These are the most common files you may encounter. But when you master those types of files you can go on and check out the other types of files.

Another way of reading files, is by typing-

File:[*,*]<command>
Once again the '*' is the wildcard.

[Creating a Directory]

To create a directory you can type at the main prompt- 'Credir'

There are 2 levels for a directory, the first level is-

Class and the second is Tvedit.

Now say we have a nice prived account, so we can have a 2 level directory. We would type-

Create Directory:[,,class,tvedit]

The Dec-10 would reply by saying-

Created Dska0:[x,x,class]Sfd/protec:775
Created Dska0:[x,x,class,tvedit]sfd/protec:755

x,x=The PPN you are using, and the Dska0 is the device.

Now we can name our directory by typing-

/Name:<what you want to call it>

Note: You don't need the brackets.

We can protect it by typing:

/Protect:<name>

There are more '/' commands so you can take a look at them by doing '/help'.

Enough of directories.

[Privs]

What almost every hacker wants when he logs onto a system is an account with privileges. If we have an account with privileges we can make our own account and do some other worth while things. Now on a Dec10 a prived account almost always begins with a '1'. Ex- 1,10. Now we can check the system status (sys) and see if we see anyone under a 1,x account. If we do then we can begin hacking the password. Now if you get in under '1,2' well that's another story. Hehe. Now say we do get in under a privileged account. Now first of all to activate our prived accounts we would type 'enable' this will either give us a '$' prompt or a '#' prompt. Whichever, it doesn't matter. We can still do what we have to do. Now let's say we want to make up a nice account, we would type-

$Build[x,x] or Create[x,x]

After we do that we can edit that PPN or if it's new make up our own.
Now, I should've mentioned this before but, if you get in on a 1,x account make sure there is not another user logged in under the same account. If it is they may change the password, but even if they are in 'exe' and may be detached
we don't want to take any chances now. Now I suggest going on in the late evening, early morning or if your home from school one day just call at noon or
so.

There are many different levels of privs, there's the operator, wheel, and CIA. CIA being the highest since you can do anything and everything.
Now if you have operator privs you can do the above which was make up an account and create a nice directory. This will also be nice when attempting to get into Decnet.

Now also if you make up a prived account, you should type-

Help Phones <as I mentioned before>

At the main prompt. You will get a list of phone numbers including the system operator's number and system managements. Now they are open usually from 10am to 5pm. Call during those hrs. and ask them if you can have a Decsystem timesharing guide. They will ask you questions like what's your name, PPN and password so have that ready. If they ask you why didn't you already receive one, just say you've just gotten a account and you were never informed about the manual.

This manual is very helpful. It will tell you commands, explain them in detail, new features, games, etc. Don't order the manual the day you get your account, wait maybe 4 days or so, then give them a call. They will usually send
it out the next day, unless they get lazy like most of the system operators do.
It's usually safe to have it sent to your house, but if you feel nervous well get it sent to another place.

[Mail Subsystem]

Sometimes you may know of a friend who also has an account on the same Dec10 you are on. Your friend may not be on the system right now, so that eliminates sending messages to him. But there is 1 alternative which is to send mail. With
mail you need the person's name. To access mail type-

Run Mail

You will then receive the prompt 'MailC', at this prompt you type-

MailC:Send

Now you will be asked questions on who you want to send the mail to. It will look something like this-

.Run Mail
MailC:Send

to:Death Hatchet
Subject:Disk Crash
Text:

Yo! My file disk got ruined with //e Writer. See ya.

Now when your finished with your text just type '.done' or '.d' on a blank line to indicate that your finish. The Dec10 will reply by saying-

Death Hatchet--Sent

-and will return you to the 'MailC' prompt. Now if you wanted to send the same message to two people you would do everything I did above except when it says 'to:' you would type-

To:Death Hatchet,The Rico

The only difference is the comma. You MUST have the comma separate the two names in order for the system not to take it as one whole name. Once the mail has been sent, the user Death Hatchet will receive it when he logs on. After he

gets the little welcome messages and his stats from when he last logged on, the
mail will automatically be read to him like this-

```
From:Carrier Culprit            Postmark:20-Mar-86-08:12:27
  to:Death Hatchet
Subject:Disk Crash

Yo! My file disk got ruined with //e Writer. See ya.
```

It will then read other pieces of mail if he has any more. If not, it will just go to the main prompt. If you want to read the mail again, go to the mail section and type 'read' instead of send. You will then be able to save it for your next call or kill it. Sometimes mail won't show up when you first logon so
go to the mail section anyway and check just in case.

On some of the older Dec10 systems mail was not used, you would just send a message. Mail was added to the Dec10 system in the mid 70's. No big deal, but just something to know. If you run mail and you don't get into the mail section
try 'run mai'. The 'run mai' is used on some of the earlier systems, but usually the system acknowledges both.

Never send violent mail to system operators, they will log you off and do away
with your account. If you do, I suggest having another account (PPN) on hand. On some of the newer Dec10 systems, you can forward mail, which you do by typing 'Frd Mail' at the 'MailC' prompt. The system will then ask you where you
want it forwarded to, their password, your password. The system operator views this and checks with both parties and he/she will leave you mail saying that it
is done. This is really being tested but I've seen it in operation on some Dec10's in 714.

[Information]

This is another handy command that can be used to your advantage. It gives you
information on jobs and PPN's. You don't get passwords but you can get some good stats. If you type 'info' or 'help info' you will get a list that would look something like this-
To look at one of the following do-- Info XXXX

Switch	Meaning
.	Information on your job
[??,??]	Information on that PPN
ALL	Information on all PPN's
ALL:LOPR	Information on all Local Operator Jobs(1,2)
ALL:OPR	Information on all Operator jobs (1,2)
ALL:ROPR	Information on all Remote Operator jobs
ALL:Users	Information on all users
Batch	Information on all batch jobs
Detached:ALL	Information on all Detached PPN'S
Detached:OPR	Information on all Detached Operator jobs
Detached:Users	Information on all Detached users
Detached:LOPR	Information on all Local Operator jobs

And the list goes on. If you want the whole list just type 'Help Info'. It will also give info on disk devices, directories, and other stuff. Some of the Dec10 systems don't support this, but you will find that most of them do.

The '1,2' which is next to the Operators are system operator accounts. I mentioned that before, so you won't get confused. Most files are kept under this account so if you get in under it you'll have a lot to do....hehehe.

[Watch]

This command will show you your stats. You will be able to toggle it. You can toggle it on which will display on the top of your screen or just look at it once. The watch will show you-

Run---which means your CPU time.
Wait--which means your elapsed time since started.
Read--number of disk blocks you have read.
Write--number of disk blocks you have written.

If you have system privs, type-

Watch[x,x]

You can watch another person if you have these privs. It will also show you information. Many operators use this so be careful in what you type.

[Other commands]

If you want to find out some information about someone type-

Who Their name job# TTY

Now I could do something like-

Who Carrier Culprit 4 #7

This is saying that Carrier Culprit is logged in on job 4 and is on TTY #7. The
monitor will also display the user's PPN, and other information dealing with his status on the system.

Now if you notice one of your friend's are on TTY10 and you want to send him a
message you can type-

Send TTY10 Congratulations on passing your exam

The user on TTY10 will receive the message and may have the capability of replying. You can also use this to meet new friends, especially a system operator who is pretty cool and can give you some accounts, but don't count on it.

If you would like to talk to someone one on one, you can type-

Talk TTY10

You will now be able to talk to each other, chat, but like I said, watch what you say sometimes, but don't get to paranoid that the system operator is

watching. Usually if the system operator is under 'Watch' or 'Exe' he may be watching a certain user. This is just basically a chat system, so have fun with
it.

 If you have a prived account go into 'enable' and type-

Whostr

 This will give information about users logged in and the directories.

 If you need the time, just type 'time'. If you have math homework just type 'aid' for desktop calculator.

Ctrl-characters
==========
ctrl-s = pause
ctrl-q = resume
ctrl-c = abort
ctrl-h = backspace

Case Commands
==========
If you support lower case type:
'Set Terminal LC'

[Decnet]

 Is supported by all Digital computers. To access it, type 'Decnet' and try to hack out the password. Decnet supports such nodes as, VMS, TOPS10 (operating system for Dec10's), TOPS20, and others. Usually system operator's accounts can
be helpful if you need a Decnet pw. Try their pw and see if it works. Usually the password to Decnet can be plain old "Decnet". Format= Set Host xxxx

[Acsnet]

 This is probably my favorite. This supports Dec10, and many other computers. When you log on to it, it will look something like this-

```
ACSNET
Fri Mar 13 19:30:23 1986
Port ID:  dialup C502  at   300 baud

dialup C502 with even parity

>
```

 Now to get a menu type '?'. It will give you a list of groupnames. To enter the Dec10 type 'Acsdec10', usually Decnet is not listed so type Decnet anyway. Other commands for ACSNET are-

```
Connect      Daytime
Hangup       Disconnect
Info         Help
Release      Resume
Set          WhoamI
```

-

Hmm. Knew I forgot something. To log off the Dec10, just type-
Bye or Kjob (kill job)

Part II: This will deal with the 1,2 PPN and advanced commands using Enable.

Have fun,

$$$$$$$$$$$$$$$$$$$$->Carrier Culprit<-$$$$$$$$$$$$$$$$$$$$

[END]
Revised Edition
(C)opyright April, 1986

==Phrack Inc.==

Volume One, Issue Five, Phile #4 of 12

+----------------------+
| Hand-To-Hand Combat |
| |
| by |
| |
| [bad boy in black] |
+----------------------+

on

^*^ 3/31/86 ^*^

This file will teach you how you can kill another person with your own two hands. The information presented here will be very helpful to the beginner and will also serve as a refresher for those of you already familiar with the subject.

I will start off by talking about basic things such as stance, what you should and shouldn't do when fighting and other information that the beginner will need to know. Then, I will give you a list of over 20 vulnerable points that one should always try attacking in a fight along with the way these points should be attacked. Finally, I will give you some more fighting tips and information on how you can continue learning about hand-to-hand combat.

^*^

Now, let me discuss some of the basics you will need to know when you are in any combat situation.

Stance

The best stance when confronting an enemy is to put your feet at shoulders length apart and your arms should be facing forward, parallel to each other and
bent at the elbows. Keep your knees slightly bent and stand on the balls of your feet.

Remember, you always want to maintain this stance when you are not striking at the enemy.

Balance

It is always important that you keep your balance. If you use the stance I have
described above, you will never have to worry about it. If by chance you do lose your balance even for a second you can kiss your ass goodbye as the enemy will probably kill you.

Aggressiveness

Always be aggressive and always attack. Don't just stand back and defend yourself against the enemy's strikes as he will end up killing you eventually. If you are not aggressive, the enemy will think you are scared and he will have

an advantage over you.

A great thing to do is yell at the enemy. This will scare the shit out of him if you start yelling at him and plus it also allows you to get more oxygen in your lungs so you will have more strength.

Natural Weapons

Your natural weapons are as follows: knife edge of either hand, the heel of your hands, your fingers folded at the second knuckle, your boot, your elbow, your knees, your teeth, your fore finger and second finger forming a "V" shape,
and your fist. These body parts alone are some of the most powerful weapons you
can use.

^*^

Since you now know the basics of fighting, let me list for you the best places where you should strike your enemy.

Temple

A sharp blow to the temple ensures instant death since there is a large artery and nerve located close to the skin surface. If you give a medium blow to the temple it will cause severe pain and concussion but a hard blow will kill the enemy instantly. The best way to strike the temple is with the knife edge of your hand or if he is on the ground you can kick him with the toe of your boot.

Eyes

The eyes are a great place to strike if you can since a good strike in the eyes
will cause temporary or permanent blindness. To blind the enemy, make a "V" shape with your fore finger and second finger and stick them into his eyes while keeping your fingers stiff. Also, you can gouge the eyes with your thumb.

Nose

The nose is another excellent place to attack. Hit the bridge with the knife edge of your hand and you will cause breakage, severe pain, temporary blindness
and even death. Or you can use the palm of your hand to strike upwards and push
the nose up into his brain. If done hard enough the nose bone will puncture his
brain and he will die.

Upper Lip

The upper lip contains a lot of nerves close to the skin surface so if you strike it with the knife edge of your hand it will cause great pain and if delivered hard enough he will become unconscious.

Mouth

If the enemy is on the ground, use the heel of your boot and strike him on the mouth. Since there are a lot of veins and arteries in the teeth there will be a

lot of blood which will frighten the enemy and he will lose concentration on defending other parts of his body.

Chin

The chin should only be struck with the palm of your hand as you can break your
fingers on the enemy's chin. Use the palm of your hand and strike the enemy with a very strong upward blow. This will cause extreme discomfort.

Adam's Apple

Usually the enemy will defend this part of his body well but if you do get the chance give it a sharp hit with the knife edge of your hand. If you hit it hard
enough you will bust his windpipe and he will die. You can also squeeze the Adam's Apple between your fingers.

Esophagus

If you have a chance to get a hold of his neck, press your thumbs into his esophagus (located below the Adam's Apple). Pushing hard will be very painful and it will block the oxygen flow to his lungs and he will die quickly.

Neck

If you give a very strong blow to the base of the neck with the knife edge of your hand you will usually break it. However, if it is not hard enough, the enemy might just be knocked unconscious so be sure to hit him in the temple or twist his neck around to be sure he is dead. The neck is the best place to hit someone if you want to be quiet as it is quick and the enemy goes down without a word.

Collar Bone

The collar bone is an extremely sensitive part of the body. A sharp blow to it with the knife edge of your hand or your elbow gives the enemy excruciating pain. Also, digging your finger into the collar bone can bring your enemy to his knees.

Shoulder

The shoulder is easy dislocated and it takes little strength to do. However, it
should be done quickly. Grab the enemy's arm and pull it behind his back and then jerk it upwards quickly. You should here a popping sound which means you have dislocated the enemy's shoulder. There are other methods of doing this but
this is the easiest.

Armpit

Although it is hard to get at, the armpit has a large network of nerves. If the
enemy is on the ground, hold up his arm and then kick him in his pit. This will
cause severe pain. However, it is not a very common place that will be struck in a fight but is good to keep in mind anyways.

Rib Cage

A strike to the rib cage with your fingers folded at the second knuckle is rather painful and if done hard enough causes severe pain and breakage. Only use your fingers folded at the second knuckle since that hurts the most.

Solar Plexus

The solar plexus is located on the chest at the little "V" shaped point where the rib cage ends. There are a large amount of nerves so a blow with the knuckle of your second finger can cause severe pain and even unconsciousness.

Floating Ribs

The floating ribs are the lower ribs located at the front and sides of the enemy's body. Use the knife edge of your hand or the heel or toe of your boot. The blow will cause pain and will stun the enemy.

Spine

A blow to the spine with the heel of your boot can paralyze or kill your enemy.
The lower spine between the enemy's kidneys is the best place to hit as that is
the least protected part of the spine. You will only be able to attack the spine when your enemy is on the ground or if his back is turned to you.

Kidneys

The kidneys have two large nerves that are close to the skin surface. If you strike the kidneys hard it will cause death. You can use a fist or the knife edge of your hand to hit the kidneys. Or a kick with the heel of your boot will
work too.

Groin

The groin is a good place to strike if you get the chance. Generally, the enemy
will protect this area the most but if you have a chance, strike it with your knee in an upward motion or with your fist. I'm sure you can imagine the pain the enemy will get from it.

Tailbone

The tailbone which is located above the anus is a very sensitive part of the body as a lot of spinal nerves are located there. Use the toe of your boot to strike the tailbone. The pain from that is unbelievably severe.

Elbow

The elbow is easy to break or dislocate. Pull the enemy's arm behind him and with the palm of your hand push his elbow inwards until it either cracks or pops. When the enemy has a useless arm, you have a great advantage over him.

Fingers

The fingers should be broken because the enemy becomes almost helpless with broken fingers. Grab the enemy's arm with one hand and with the other hand push
the fingers upwards until they snap. It is only necessary to break the first two fingers. It is also helpful in breaking a grip.

Knee

You can destroy the knee by kicking it with the side of your boot in an upward motion. This will rip the ligaments and the cartilage. This will cause unbelievable pain and make it impossible for the enemy to move around. Once a knee has been ruined, you will have a great advantage over the enemy.

Ankle

If the enemy is on the ground, get a hold of his ankle and twist it until it snaps. This will make it almost impossible for him to walk and he will then be easy to kill.

^*^

Let me talk about some more important things you should remember when you are fighting somebody.

Tactics

Always try to throw your enemy off balance. You can do this by charging the enemy and pretending to strike him. This will make him flinch and lose his balance.

Always look for a weak spot and attack it. Whenever he leaves a vulnerable part
of his body unprotected attack it with all your strength. By doing this, he will then try to protect the part of his body that you just struck thus leaving
even more unprotected parts open.

Use any available object that you can. By this I mean throw sand in his eyes, block his strikes by hitting him with a large branch, or any other kind of available material that can be used as a weapon against him.

Foul Play

In a life or death situation there is no such thing as foul play and there are no rules either. Although hitting someone in the groin is considered a cheap shot in high school, it is a very effective way of destroying your enemy. Just hit him where you can and kick him when he's down. That way, he will never get back up again.

^*^

I have now explained to you the basics of fighting and the best places to attack your enemy on his body. Just because you have read this file doesn't mean you will be able to go out and kick somebody's ass in. These methods take a lot of practice in order to do them properly.

If you enjoyed this file and would like to practice these methods get a partner
who is also interested in this and work on each type of strike and kick. When you first start out, go slowly and remember that these methods are deadly and do not require much force to be effective so take it easy on your partner.

Some of you may decide that practicing is not enough and you would like to learn more than what I have told you in the above. Well, there are several good
books with illustrations on this subject which go into much more detail than I ever could in this file. The book I used mainly to write this file was "The

Marine Corps Field Manual on Physical Security". You can get this book through a good book store or if you happen to know a marine, he can get you a copy very
easily.

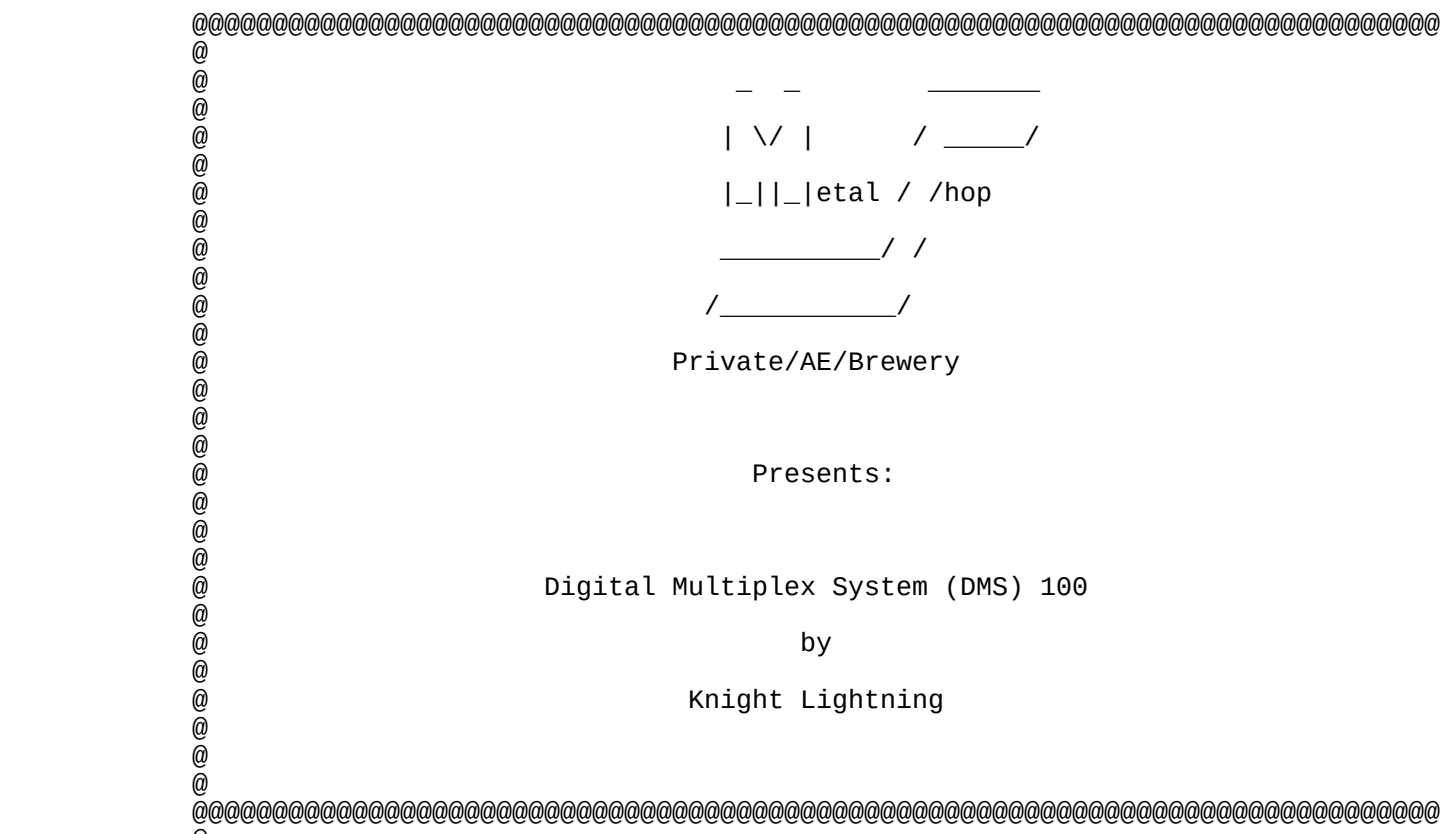
There are also camps where you can go for 1-2 weeks to learn all sorts of things like this such as firing weapons, detailed hand-to-hand combat, doing raids on enemies and all sorts of other stuff like that. The instructors that teach these programs are well trained and have had years of experience with this. However, usually you have to be 18 years or older to get into these programs and you have to be very serious about it as well. This is not one of those programs where you can say "Time-out, I need to rest." They don't stop just to suit you. To get more information about these programs, you can usually
find out about them in magazines like "Soldier of Fortune" and other magazines with similar theme.

^*^

Well, that's it for now. Perhaps in the future I can discuss the fun stuff like
fighting people with knives and all the other lethal weapons you can use in a fight. If you liked this file, let me know and I will continue on with this subject.

==Phrack Inc.==

Volume One, Issue Five, Phile #5 of 12



This file is of course about DMS 100. Expect full length files about the other variations of DMS (DMS 200 & 250) coming a later date. Much of the information in this file was obtained from manuals acquired from Jester Sluggo. Note: IBN stands for Integrated Business Network.

DMS-100

The DMS-100/IBN consists of electronic business sets and standard telephones, data units, and attendant consoles, all located on the customer's premises; and
DMS-100 digital switching, and support hardware/software, located at the telephone company's premises. Together they create an integrated business communications network that provides an unparalleled combination of features and benefits.

- DMS-100/IBN integrates voice and data in a total business communications system.
- Effectively serves all sizes of organizations, from small businesses using only a few lines, to the most complex network systems with up to 30,000 lines.
- The IBN system monitors and controls its own operations automatically; diagnoses problems; and in some cases, does its own repairs.

- Fully modular, to meet present needs, and accommodate new features as they are needed.

- Cost effective: Helps control communications costs through more efficient use of facilities; centralization of attendant service where needed; Call Dial Rerouting (CDR) to control and restrict long-distance calling; and network management.

- Worry free operation-Northern Telecom's DMS-100 digital switches are backed up by highly trained telephone company personal.

Some of the other features that DMS 100 has include:

- Automatic Route Selection - automatically routes long distance calls over the most economical route available.

- Station Message Detail Recording - provides a detailed record of long distance charges, including the originating number, time, and duration, authorization code, etc.

- Direct Inward System Access (DISA) - enables company personnel to use cost-saving company facilities for long distance calling, even from outside the company.

System Features and Benefits

Note: I will list all the features, but I will only go into detail about the important ones.

ATTENDANT CONSOLE

Call Waiting Lamp
Loop Keys - There are 6 loop keys, each with its associated source and destination lamp to indicate the calling and called party states.
Alphanumeric Display
Multiple Directory Numbers
Feature Keys - Up to a total of 42. Some of them could be used for Speed Calling and Paging System.
Incoming Call Identifier
Exclude Source/Exclude Destination - privacy keys
Signal Source/Signal Destination: Release Source/Release Destination

Console Features

Access to paging	Call hold
Call detail entry	Remote console
Call Selection	Console display
Camp-on	Automatic recall
Conference - 6 port	Two-way splitting
Non-delayed operation	Attendant transfer
Locked loop operation	Busy verification of lines
Manual and automatic hold	Multiple console operation
Busy verification of trunks	Switched loop operation
Trunk group busy indication	Uniform call distribution form queue
Multiple listed directory numbers	Control of trunk group access
Secrecy	Night service
Serial call	Speed calling

Lockout
Position busy
Through dialing
Delayed operation
Interposition calling

ELECTRONIC BUSINESS SETS

LCD Indicators
Call Forwarding
Automatic Line
Call Pick-up
Ring Again - automatically redials busy numbers until they are free
Multiple Directory Numbers
Intercom
Speed Call
Call Transfer/Conference
On-Hook Dialing

Additional Programmable Features

Automatic Hold
Listen-on Hold
Multiple Appearance Directory Numbers (MADN)
 - Single Call Arrangement
 - Multiple Call Arrangement
Privacy Release
Tone Ringing with Volume Control
End-to-End Signaling
Call Park
Make Set Busy
Malicious Call Trace
Busy Override
Attendant Recall
Call Waiting
Stored Number Redial
Private Business Line
32 Character Alphanumeric Display

DATA UNIT

The DMS-100/IBN Data Unit makes information accessing as easy to learn and to use as the telephone. It can be used as a "Standalone" or attached to the Business Set or standard telephone, for integrated voice and data telephone telecommunications.

Transmits over simple 2-wire loops, at speeds of up to 56 kb/s, using Northern Telecom's proprietary Time Compression Multiplexing technology; Compatible with
existing computer and data terminal equipment, and is available in different low-speed and high-speed models, to suit existing terminal capacity.

Benefits

- Combines with Business Set or standard telephone, to provide integrated voice/data communications.

- Your data unit and telephone can operate together simultaneously or totally independent of each other.

- Fully digitalized, eliminating bulky analog modems.

o Ring Again (constant redial on busy numbers)

o Speed Calling

For further information contact:

Digital Switching Systems Sales
Northern Telecom Inc.
P.O. Box 13010
4001 East Chapel Hill -- Nelson Highway
Research Triangle Park
North Carolina 27709
Tel: (919) 549-5000

Switching Group Sales, Department S-70
Northern Telecom Canada Limited
8200 Dixie Road, P.O. Box 3000
Brampton, Ontario
L6V 2M6
Tel: (416) 451-9150

==Phrack Inc.==

Volume One, Issue Five, Phile #6 of 12

+=+=+=

Ok, take the matches, and there should be a 2 colored tip on the end. Well, cut the top layer off (this should be done with a razor blade) carefully, as to
not set the matches off. Ok. Got that? Good, now, take about, oh, four or five heads, or if you're feeling kind of dangerous, and can fit them, try six. Put the heads <white part> into the space that is between the other side of the
bolt and the nut. Now, carefully, take the other bolt and screw it down kind of tight onto the other side. You now should have the 2 bolts connected by the
nut, and the matches in between this whole hardware contraption.

Now what??!?

Take this thing, and throw it at something solid, and hard, like the street, for instance, and be sure you throw it kinda hard, and kinda far. These can be
a lot of fun, and only take a second to build.

Received: (from LISTSERV@PSUVM for TK0EEE1@UCLAMAIL via NJE)
(LISTSE00-7268; 153 LINES); Tue, 19 Dec 89 17:45:31 CST
Date: Tue, 19 Dec 89 17:45 CST
To: TK0EEE1
From: LISTSERV@PSUVM

==Phrack Inc.==

Volume One, Issue Five, Phile #6 of 12

```
+=+=+=
```

==Phrack Inc.==

Volume One, Issue Five, Phile #7 of 12

Jester Sluggo presents
an insight on
Wide-Area Networks
Part 1

Part 1 contains information on ARPANET and CSNET.
Part 2 contains information on BITNET, MFENET, UUCP and USENET.
It is best if you read both files to better understand each other.

These files will cover general information on wide-area networks, (I.E. ARPANET, CSNET, BITNET, MFENET, UUCP and USENET), but may contain information in relationship with other networks not emphasized in these files. These files are NOT a hacker's tutorial/guide on these systems.

ARPANET

ARPANET. The ARPANET, which is a major component of the NSFnet [National Science Foundation Network], began in 1969 as an R&D project managed by DARPA [Dept. of Defense Advanced Research Projects Agency]. ARPANET was an experiment in resource sharing, and provided survivable (multiply connected), high bandwidth (56 Kilobits per second) communications links between major existing computational resources and computer users in academic, industrial, and government research laboratories. ARPANET is managed and funded by by the DCA [Defense Communications Agency] with user services provided by a network information center at SRI International.

ARPANET served as a test for the development of advanced network protocols including the TCP-IP protocol suite introduced in 1981. TCP-IP and particularly IP, the internet protocol, introduced the idea of inter-networking -- allowing networks of different technologies and connection protocols to be linked together while providing a unified internetwork addressing scheme and a common set of transport of application protocols. This development allowed networks of computers and workstations to be connected to the ARPANET, rather than just single-host computers. TCP-IP remain the most available and advanced, non-vendor-specific, networking protocols and have strongly influenced the current international standards of activity. TCP-IP provide a variety of application services, including remote logon (Telnet), file transfer (FTP), and electronic mail (SMTP and RFC822).

ARPANET technology was so successful that in 1982, the Dept. of Defense (DOD) abandoned their AUTODIN II network project and adopted ARPANET technology for the Dept. of Defense Data Network (DDN). The current MILNET, which was split form the original ARPANET in 1983, is the operational, unclassified network component of the DDN, while ARPANET remains an advanced network R&D tested for DARPA. In practice, ARPANET has also been an operational network supporting DOD, DOE [Dept. of Energy], and some NSF-sponsored computer science researchers. This community has come to depend on the availability of the network. Until the advent of NSFnet, access to ARPANET was restricted to this community.

As an operational network in the scientific and engineering research community, and with the increasing availability of affordable super-minicomputers, ARPANET was used less as a tool for sharing remote computational resources than it was for sharing information. The major lesson from the ARPANET experience is that information sharing is a key benefit of computer networking. Indeed it may be argued that many major advances in computer

systems and artificial intelligence are the direct result of the enhanced collaboration made possible by ARPANET.

However, ARPANET also had the negative effect of creating a have--have not situation in experimental computer research. Scientists and engineers carrying out such research at institutions other than the twenty or so ARPANET sites were at a clear disadvantage in accessing pertinent technical information and in attracting faculty and students.

In October 1985, NSF and DARPA, with DOD support, signed a memorandum of agreement to expand the ARPANET to allow NSF supercomputer users to use ARPANET to access the NSF supercomputer centers and to communicate with each other. The immediate effect of this agreement was to allow all NSF supercomputer users on campuses with an existing ARPANET connection to use ARPANET. In addition, the NSF supercomputer resource centers at the University of Illinois and Cornell University are connected to ARPANET. In general, the existing ARPANET connections are in departments of computer science or electrical engineering and are not readily accessible by other researchers. However, DARPA has requested that the campus ARPANET coordinators facilitate access by relevant NSF researchers.

As part of the NSFnet initiative, a number of universities have requested connection to ARPANET. Each of these campuses has undertaken to establish a campus network gateway accessible to all due course, be able to use the ARPANET to access the NSF supercomputer centers, from within their own local computing environment. Additional requests for connection to the ARPANET are being considered by NSF.

CSNET

CSNET. Establishment of a network for computer science research was first suggested in 1974, by the NSF advisory committee for computer science. The objective of the network would be to support collaboration among researchers, provide research sharing, and, in particular, support isolated researchers in the smaller universities.

In the spring of 1980, CSNET [Computer Science Network], was defined and proposed to NSF as a logical network made up of several physical networks of various power, performance, and cost. NSF responded with a five year contract for development of the network under the condition that CSNET was to be financially self-supporting by 1986. Initially CSNET was a network with five major components -- ARPANET, Phonenet (a telephone based message relaying service), X25Net (suppose for the TCP-IP Protocol suite over X.25-based public data networks), a public host (a centralized mail service), and a name server (an online database of CSNET users to support transparent mail services). The common service provided across all these networks is electronic mail, which is integrated at a special service host, which acts as an electronic mail relay between the component networks. Thus CSNET users can send electronic mail to all ARPANET users and vice-versa. CSNET, with DARPA support, installed ARPANET connections at the CSNET development sites at the universities of Delaware and Wisconsin and Purdue University.

In 1981, Bolt, Beranek, and Newman (BBN) contracted to provide technical and user services and to operate the CSNET Coordination and Information Center.
In 1983, general management of CSNET was assumed by UCAR [the Univ. Corporation for Atmospheric Research], with a subcontract to BBN. Since then, CSNET has grown rapidly and is currently an independent, financially stable, and professionally managed service to the computer research community. However, the momentum created by CSNET's initial success caused the broad community

support it now enjoys. More than 165 university, industrial, and government computer research groups now belong to CSNET.

A number of lessons may be learned from the CSNET experience.

1) The network is now financially self-sufficient, showing that a research is willing to pay for the benefits of a networking service. (Users pay usage charges plus membership fees ranging from $2000 for small computer science departments to $30,000 for the larger industrial members.)

2) While considerable benefits are available to researchers from simple electronic mail and mailing list services -- the Phonenet service -- most researchers want the much higher level of performance and service provided by the ARPANET.

3) Providing a customer support and information service is crucial to the success of a network, even (or perhaps especially) when the users are themselves sophisticated computer science professionals. Lessons from the CSNET experience will provide valuable input to the design, implementation, provision of user services, and operation and management of NSFnet, and, in particular, to the development of the appropriate funding model for NSFnet.

CSNET, with support from the NSFnet program, is now developing the CYPRESS project which is examining ways in which the level of CSNET service may be improved, at low cost, to research departments. CYPRESS will use the DARPA protocol suite and provide ARPANET-like service on low-speed 9600-bit-per-second leased line telephone links. The network will use a nearest neighbor topology, modeled on BITNET, while providing a higher level of service to users and a higher level of interoperability with the ARPANET. The CYPRESS project is designed to replace or supplement CSNET use of the X.25 public networks, which has proved excessively expensive. This approach may also be used to provide a low-cost connection to NSFnet for smaller campuses.

/
\
/ luggo !!

Please give full credit for references to the following:
Dennis M. Jennings, Lawrence H. Landweber, Ira H. Fuchs, David J. Faber, and W.
Richards Adrion.

Any questions, comments or Sluggestions can be emailed to me at Metal Shop, or sent via snailmail to the following address until 12-31-1986:

J. Sluggo
P.O. Box 93
East Grand Forks, MN 56721

==Phrack Inc.==

Volume One, Issue Five, Phile #8 of 12

- Short-Wave Radio Hacking -

by

The Seker

Every day, tons of information is exchanged over the air waves. I have found news agencies, military computers, businesses, and even hacks.

The standard method of exchange is called RTTY (Radio Teletype). It usually is used at 66/7 words per min. Instead of using ASCII, Baudot, a 5 bit character set is more widely used. There are many variations of it in use also.

There are many other types of transmission standards besides RTTY that are commonly used. A few of the known:

FAX (Facsimile)

Helshcrieber- it's used to transmit pictogram-type alphabets (i.e. Chinese, Jap, etc.) instead of the American letters.

SSTV- is similiar to Viewdata. Used for transmitting high-resolution pictures mixed with text.

To start, you'll need to buy (card) a receiver (with a coverage of no less than 500 kHz-30 MHz and a resolution greater than 100 Hz) and a high quality antenna. These can usually be found at electronics stores. You will also need
to get an interface and some RTTY software for your particuliar computer. Look
in magazines like 'Amatuer Radio' or 'Ham Radio Today' for more information on that shit. Another good place to check is a CB store.

NEWS AGENCIES-

From these you can find all sorts of crap. You may even intercept a story being sent to the presses. They tend to operate at 66/7 words a minute (50 baud). A few of the more common 'fixed' bands they transmit over are:

at kHz:

3155-3400	3950-4063
9040-9500	12050-12330
13800-14000	15600-16360
19800-19990	25210-25550

An easy way to tell if you have located a news agency is by some lame transmission being continuosly repeated.

i.e. 'RYRYRYRYRYRYRYRYRYRYRY' etc.

This is done so they can keep their channels opened for reception.

CONFERENCES-

Another thing I found interesting was the channels that the amatuers congregated around. I frequently ran into people from foreign countries that couldn't even speak English. I even ran into other hackers from all over!
A few of the more popular spots that amatuers hang out are:

at kHz:

3590 14090 21090 28090

at MHz:

432.600 433.300

at VHF/UHF:

144.600 145.300

PACKET RADIO-

A new development in radio transmission is the packet radio. From what I've seen, it's just like digital packet switching networks, i.e. Compuserve, Telenet, Tymnet, etc.; except slower.
In fact, Compuserve has been researching a way to transmit its services cheaply.

--tS

This has been written exclusively for

---Metal Shop Private---

==Phrack Inc.==

Volume One, Issue Five, Phile #9 of 12

Mobile Telephone Communications

By Phantom Phreaker

Presented by The Alliance
(618)667-3825

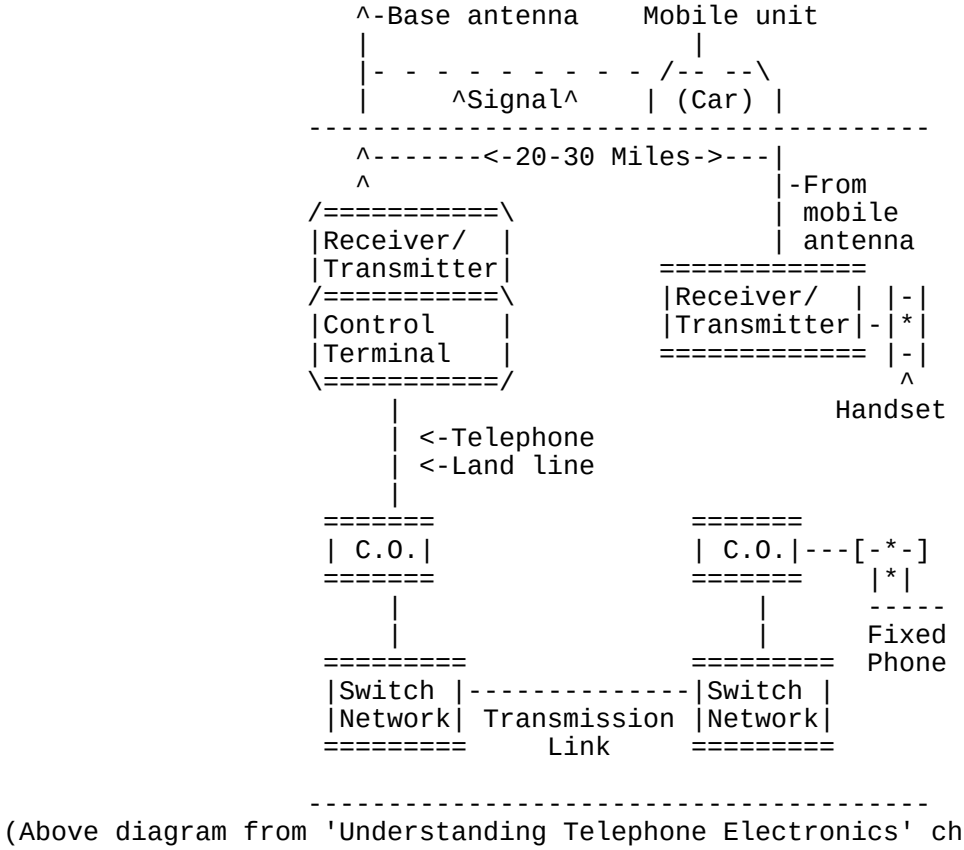
Mobile telephone communications is not the same thing as Cellular. Mobile telephone service is not as advanced as Cellular, and not as efficient. Mobile telephone service limits the number of customers sharply, while Cellular is designed to solve the problems of Mobile telephone service.

The signals for Mobile communications are sent by high-power transmitters and antennas that provide an area of approx. 20-30 miles with service.

A base unit of a Mobile communications system transmits and receives on different frequencies at the same time. Typical power for the radio base station transmitter is 200-250 watts.

Mobile telephone facilities tie in with the normal fixed-position telephone system, however base units can be owned by a Radio Common Carrier (RCC). RCCs running mobile telephone systems are charged by the telephone company for use of the normal phone system.

DIAGRAM:



(Above diagram from 'Understanding Telephone Electronics' chapter 10.)

As you can see from the above diagram, calls placed from the Fixed position telephone are routed through a Central Office as normal, through a Switch Network, to another Switch network, and to another CO. From the second CO (nearest to the Mobile unit), the signals are sent on a telephone line to the control terminal, to the receiver, then to the base unit (antenna). From the base unit, the radio signals are sent to the site of the mobile telephone.

Calls from the mobile telephone operate in the same manner. An idle radio channel is selected (like seizure of a trunk for a LD call) and the signals are sent over the mobile network.

If no channel is available for use, then a busy indication is triggered (similar to a re-order). If a channel is available, the customer will be prompted with a dial tone, similar to normal fixed-position telephone service.

The area that this would work in is called the subscriber's home area. When a mobile telephone service subscriber leaves the service area, he is then referred to as a Roamer. Since the mobile unit is out of the service area, special preparations have to be made to continue communications to/from that mobile unit.

SIGNALLING

Mobile signalling tones are selected (like touch tones) to avoid possible reproduction of the signalling tone on the voice link, to cause a signalling mistake. The IMTS (Improved Mobile Telephone Service) uses in band signalling of tones from 1300Hz-2200Hz. Another method of signalling is the MTS (Mobile Telephone System). MTS is older than IMTS, and MTS uses in band signalling of tones from 600Hz-1500Hz, and some use 2805 Hz in manual operation.

CALL COMPLETION

In this instance, let's say a call is being placed from a normal telephone to a Mobile unit. First off, the base station selects one idle channel and places a 2000Hz idle tone on it. All on hook Mobile units active in that service area find and lock onto the channel that carries the 2000Hz idle tone. Now each Mobile unit listens for it's specific number on that channel. When an idle channel becomes busy, a new channel is selected for use, and the process is repeated.

Now the caller's call is sent through the telephone network the same way as a normal telephone call. When this call reaches the control terminal, the terminal seizes the already marked idle channel (with every on-hook mobile unit listening to it) and applies a 1800Hz seize tone. This tone keeps other mobile units from using it to complete other calls. The called number is outpulsed over the base station transmitter at ten pulses per second, with idle tone represented as a mark, and a seize-tone represented as a space.

Since every idle mobile unit is waiting on that channel, they compare the number being outpulsed with their own number. If the first digit of the called mobile unit is three, and a specific mobile unit 'listening' on the channel has a first digit of four, it stops listening to that channel, and moves to the next channel with 2000Hz applied.

When the mobile unit receives the correct destination number, all other mobile units are no longer listening on that particular channel. When the 7 digit number is received, the mobile supervisory unit turns on the mobile transmitter and sends an acknowledgement signal (2150Hz guard tone) back to the control terminal. If this signal isn't received in three seconds after outpulsing, the seize tone is removed from that channel, and the call is dropped. If the signal is received at the control terminal, then the mobile phone will ring (standard two seconds on, four seconds off). If the mobile unit

being called doesn't answer in forty five seconds, the call is also dropped. When the person answers the mobile phone and takes it off hook, the mobile supervisory unit sends a connect tone of 1633Hz, for an answer signal. When this is received by the control terminal, the ringing stops, and a voice path between the two phones is established. When the mobile subscriber hangs up, a disconnect signal is sent which consists of alternating disconnect/guard tone (1336Hz and 2150Hz respectively) signals. Then the mobile unit begins searching
for another idle channel, and readies itself for more calls.

For an outgoing call placed by the Mobile subscriber, the mobile unit must already be locked on the idle channel. If the unit is not, a warning light will
flash advising the user of the problem. This is similar to a re-order signal.

If the unit is already on an idle channel, the calling number will be sent to the control terminal for billing purposes.

CELLULAR TELEPHONES

To improve over the problems of mobile telephone service such as low amount of
users, high price, etc. AT&T invented the Cellular Concept, or the AMPS (Advanced Mobile Phone System). This is the cellular phone concept that is used
in major cities. Los Angeles, Ca. currently has the largest cellular communication system in the world.

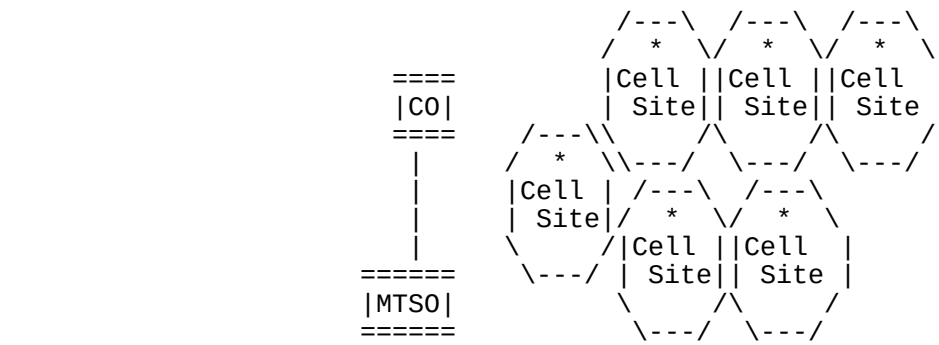
Calls sent to cellular telephones are sent through the MTSO (Mobile Telecommunications Switching Office). The MTSO handles all calls to and from cellular telephones, and handles billing.

All incoming calls from the MTSO are sent to a Cell site in each cell, to the actual cellular telephone. The major difference between mobile and cellular is that cellular can use the same channel many more times than a mobile telephone system can, providing more customers and making the service less expensive.

Once a vehicle goes out of range of one cell site, the signal is transferred immediately, with no signal loss, to another cell site, where the call is continued without interruption. This is called a Cellular hand-off.

Cellular communications areas are divided up into several cells, like a honeycomb.

DIAGRAM



More cell sites are used for the area they are needed for. The signals are sent from the MTSO to the each cell site. So if you were travelling in the cell
site to the far left, the signal from the MTSO would be sent to that cell. As you move, the signal is moved.

Here is a quote from AT&T's Cellular Telephones pamphlet.

'AT&T cellular phone transmission sounds as good as your home and office phone. Basically it's a simple concept. Each metropolitan area is divided into sectors which form a honeycomb of cells. Each cell incorporates its own transmitter and receiver which connects to the local phone network.
As you drive from cell to cell, sophisticated electronic equipment transfers or 'hands off' the call to another cell site. This automatic sequence maintains
service quality throughout the conversation without interruption.'

I hope this file has been of some assistance to anyone who is curious about the more technical aspects of the telephone system.

References

Understanding Telephone Electronics-by Texas Instruments 1983
TELE Magazine issues three and four
AT&T Mobile communications pamphlet
AT&T Cellular concept pamphlet

-End of file-
4/14/86

==Phrack Inc.==

Volume One, Issue Five, Phile #10 of 12

=-=-=-

the following letter:

Dear Sirs, 4/1/86

My name is Taran King, as you so easily researched, and I used to run Metal Shop, an electronic bulletin board system. I currently run a private line for personal friends of mine, and if asked, I distribute "general files" for them. The fact that I distributed the file is hardly the point. I merely obtained it from the authors of the file and distributed it to other sources, who apparently distributed it other places. If I am responsible for this file, I believe you should find a number of other authors also.

It is not only this file that you have written me about that the information about the "secret" to picking Master locks is included in, but also a number of other files that have been circulating for years. It is old information, someone just re-published it. Although on this topic, I am not well informed, I believe it is legal to print information on such a topic. We do not condone the actions promoted by the files, but merely inform the public on the topic of this. I hate to run on, but I wish to make my point as clearly as possible.

If I, being one of the people it was passed through, am responsible for the crime rate today of people picking Master, American, or any other company's locks, then I believe anyone who has the file, or has read books should be arrested on this. I believe Paladin Press publishes a number of books on this topic. I have seen one of the "Picking Master Locks in 3-Easy Steps!" type books and as far as I know, it's still in publication and distribution.

I hope I'm not sounding disrespectful or condescending, but it annoys me to a great degree when I must be questioned by my father about a letter that has come in the mail from a law firm in New York. Please expect a letter from him inquiring upon the topic that you have written me on. If you wish to have further discussion, feel free to call me at my voice line whenever you want to at (314) XXX-XXXX. Don't play funny like you did with the letter and reverse the charges or something entertaining like that please.

Sincerely,

Taran King

If any of you are wondering as to how they found Taran, well CN/A is not exclusively for phone phreaks and the number to Metal Shop was published in Phrack I in most of the files. My theory about how they found this file is:

A. Some agent type is looking around (hell we all know they are out there), he sees the file and passes it on to Master Lock Company;
B. Some rodent dork type whose dad works for Master Lock Company sees it and says, "Hey Dad, look, this is really neat!"

I guess it really doesn't matter... Knight Lightning

Lex Luthor Speaks About TWCB Sunday March 22, 1986

The following is a message from Lex Luthor regarding TWCB Inc.

-
It has been brought to my attention that TWCB Inc. is "throwing around large amounts of BS involving me". I have NEVER spoken to them, not on a conference, bbs, or anything.

They have no affiliation with The Legion of Doom phreak group, nor The Legion Of Hackers hack group. Any references they make regarding me or any member of LOD or LOH should be disregarded since it's probably bullshit.

TUC is working on Project Educate but there are no dates as of yet when an issue will be released. He scrapped the old first issue and is working on a better quality newsletter. I don't really have anything to do with Project Educate except that I may contribute some material.

I just thought I would clear this up and if anyone hears anything different, please send me email with the information.

One other thing that is on my mind is how some phreaks/hacks put down 2600 Magazine as not being that great, not providing enough technical info, or providing too technical, etc. Well compared to the other rags out there, 2600 does a pretty damn good job and are very consistent, you never have to worry about getting ripped off by them, and they are trustworthy. I don't agree with some of the ways they do things, but overall they are pretty good.

I just wanted to get a few things off my chest.

Lex

_

TRASk, Animator, Ogre Ogre busted 408 Under Siege

This all happened towards the end of the week after the Phoenix Phortress Sting
Operation.

TRASk the sysop of Shattered World Elite, carded an IBM PC. The person whose house it was to be delivered, happened to be at home when it arrived. The owners promptly called the police who then set up a stake out and waited for an
unsuspecting TRASk to waltz over and pick it up. TRASk did and of course was caught red handed.

Walking up to the house but staying on the street was the Animator. He didn't like the looks of the situation and didn't stop walking. He went to the home of BelGarion and Ogre Ogre (brothers). Unknown to him he had been followed over. Since he had cut school that day he stayed over there until 4PM. BelGarion and Ogre Ogre went to Animator's house and took all his computer equipment and illegally carded shit. They hid it all in their house. Minutes after Animator left BelGarion's home, he was picked up by the police. He was then taken to Juvenile Detention where he found TRASk.

Meanwhile the police went to TRASk's house first and took all his shit including the bbs, then over to Animator's. When they got to Animator's house and couldn't find anything, his little brother told them that BelGarion and Ogre Ogre took everything. They then went to BelGarion's house where they found
not only Animator's carded material but BelGarion's and Ogre Ogre's as well.

The four of them spent the weekend together in Juvenile Detention.

The charges included:

o Fraudulent use of a credit card
o Grand theft
o Possession of stolen property

The merchandise found at BelGarion's was in excess of $3,000.

Being that BelGarion is 18 years old, Ogre Ogre, his younger brother, took full
responsibility for the crimes. As a result the charges against BelGarion were dropped.

The court case is expected to take place in mid-April 1986.

The interesting part about this story is that TRASk and the others were members
of the Nihilist Order. This group had most of its members busted or under surveillance already due to the Phoenix Phortress Sting Operation in Fremont, California. Is there a connection?

BelGarion says no, and that the Nihilist Order was really a loosely connected bunch. It was however started by TRASk and The Highwayman.

TRASk was released with a $100 fine and probation and 100 hours of community (civil) service work. His bbs, The Shattered World Elite, will be going back up sometime in the future.

For information about the Phoenix Phortress Sting Operation see Phrack World News Issue III.

Information provided by BelGarion 408 in an interview with Knight Lightning

---

Robin Hood and The Sultan Busted 408 Under Siege

This event took place around the last week of March in California, the 408 area.

Robin Hood had sprained his ankle at a wrestling meet and as a result was laid up at home for several days. On one such day, he awoke at 1:30 PM in the afternoon to hear people outside his house, trying to force his doors opened. Hobbling around on his crutches, he made it to the kitchen where he ran into three police officers, two special investigators, and one guy from PacBell Security.

His first cry was, "You had better have a warrant!" Sure enough they did. He noticed MCI codes and dialups written on it as well as passwords to TRW. (Editor's Note: Obviously what they were looking for.) They went to his room and went through his computer disks (one of which was labeled phreaking and hacking, they jumped for that one), printouts, notebooks, and anything else they could find. They took everything including his modem, printer, phone, and
computer.

Among what was confiscated were printouts of Phrack Issues I-III, Hack Newsletter (all issues to date), tons of other G-philes, and Lex Luthor's Hacking Cosmos series. Also taken were all of his board numbers he was on and all his passwords. Luckily for Metal Shop PRIVATE, he had not yet received the new general password. Boards that should be wary include the Alliance and P-80.

His charges include:

o Annoying Calls (Scanning Prefixes)
o Defrauding the phone company
o Illegal entry (Hacking)
o Scanning MCI dialups (I don't know what the legal name for that would be)

His and Sultan's court case comes up on April 18th 1986 1:00 PM.

As for the Sultan, upon being busted, Robin Hood tried to get in touch with him at school, not knowing that the group that had paid him a visit had come from the Sultan's earlier around 11:30 AM. When he finally did reach him around 4:00 PM after school at swim practice, it was much too late. Sultan's dad supposedly held a government related job. (I have no idea if it was a political one or not).

The police had grabbed everything Sultan had as well, including his phone. Since his bust he has had his phone line disconnected.

Robin Hood said that he was told that he had been under surveillance for 2-3 months previous to his arrest.

He also recalled that the police had a third warrant for someone in a different town. He did not recognize the name, nor did he hear anything about it later.

(Editor's Note: Their accounts on Metal Shop PRIVATE were removed long ago, so MSP users don't be worried.)

Information provided by Robin Hood during an interview with Knight Lightning

---

TWCB: Peter Arrested Again TAP Trouble

In the last week of March, while on spring break, Peter of TWCB Inc. was arrested (or maybe just picked up) for leaving his home while under a court order to stay confined there under his mother's reconnaissance.

He was picked up by the same detective that busted TWCB Inc. in the first place. Evidently he had been staking out their condominium for some time.

Not only does this add to their LARGE record and current charges, but it will be used to show the court that TWCB's mom has no control over them. This will hurt their defense.

Many questions have arisen about the upcoming court case against TWCB. Most notably, how will they be able to publish TAP Magazine with such a record and

constant surveillance? Since their bust was basically non-phreak/hack related maybe there is no real reason to fear any problems arising of information trading for a lighter sentence if (when) found guilty.

However, their bust also concerned fraudulent use of a credit card. What if that were to be tied in to phreak/hack bulletin boards?

Since the topic of TWCB has already been brought up, I'd like to mention some of the other things that have been going on concerning them.

Fights breaking out between them and Sigmund Fraud have cleared up. This does not necessarily mean that they will not resume. Fights with Slave Driver that led to their being kicked off of Stronghold East Elite, have also cleared up. Not wanting to have a reputation for kicking people off SEE for personal reasons, Slave Driver has allowed TWCB to return. It is not yet known if they have done so as of yet.

On the other hand, with their co-sysop access, TWCB kicked Broadway Hacker off of Spectre III (Which is sysoped by The Overlord of 815). He in turn kicked them off of the Radio Station BBS. Hostilities raged between the two, but Broadway Hacker publicly apologized on Metal Shop (and I suppose on several other bbses as well) to TWCB, and asked them to remove their vulgar posts about
him. TWCB made no comment.

Broadway Hacker did kick TWCB off The Radio Station. Later he welcomed them back on, but now with their refusal to call, his invitation no longer exists.

SBS Acquisition Completed March 1986

On February 28, MCI completed its acquisition of Satellite Business Systems from IBM in exchange for approximately 47 million shares of MCI Common stock, of 16.7 percent of the 282 million shares now outstanding. The Federal Communications Commission (FCC) approved the transfer to MCI of authorizations held by SBS on February 14. The transaction was announced as an agreement in principle on June 25, 1985.

The majority of SBS employees have joined MCI, bringing MCI's employment to 14,800.

Initially, for SBS's 200,000 customers, the acquisition brings no change in service or rates. Eventually, the SBS system will be combined with MCI's more extensive domestic and international network.

Taken from MCI World, March 1986

==Phrack Inc.==

Volume One, Issue Five, Phile #11 of 12

=-=-=-

places (most notably Stronghold East Elite) and was confirmed in interview with
Lex Luthor by Knight Lightning on April 4, 1986.

The Twilight Zone will be back up in 1-2 weeks. Those who Marauder wants on will be contacted with all the new logon info, along with a number to reach it at. He has been doing some mods to the software so the board has been down. Silver Spy, Sysop of Catch-22 has had some phone problems and as soon as the phone company fixes it he will have it back up. Both boards did go down for a few days after the Doctor Who bust, but after we found out why he was busted, the boards went back up.

The Secret Service came to Who's house and took everything, he was not home at the time, but after 1-2 days, they finally got around to questioning him. As you know, the Secret Service has been doing a lot of credit card investigations. Initially Pit Fiend of CA was busted for carding (Editor's Note: See last issue's quick notes as to Pit Fiend) and at the time he was speaking w/Who from time to time, thus some believe Who's bust was a result of P.F. leaking info to the S.S.

LOD/H was not shaken up too much from Who's bust mainly because it was not Phreak/Hack related, merely credit related which LOD/H is not involved in. Who did not card anything, but we believe the S.S.'s motive for busting him was use
of TRW. Incidentally, Who had a DNR on his line for 7 months some say it was for over a year, but either way, its a hell of a long time! That's about it, anyone need specific details, or heard anything otherwise let me know.

Lex

Information provided by Lex Luthor

(Editor's Note: Lex Luthor also mentioned that Dr. Who is being sued by AllNet)

2300 Club Members Busted
Cleveland

Two have been caught for fraudulent use of a credit card and one has been arrested for car theft.

The 2300 Club is now being compared and treated as a miniature mafia by local authorities. This is mainly for other crimes including the blowing up of cars.
King Blotto was, at one time at least, a member of this group. There is absolutely NO information regarding King Blotto as being busted or as still being a member of the 2300 Club.

New Phreak/Hack Group April, 6 1986

The Dark Creaper (916), Brew Associates (215), Major Havoc (301), and one other
whose handle is unknown to me at the current time are forming a new phreak/hack

group. Its name is "The IBM Syndicate". They are currently looking for members to join. Their bulletin boards, which are currently more or less public, will very soon be going private, thus making it harder to become a member. Eventually the group will have 2 bbses and 2 AEs. Mainly for the exchange of files and IBM kracked wares. All of these bbses will be run on of course IBM, and I assume that having an IBM is a requirement to become a member.

Information provided by Dark Creaper through interview by Knight Lightning

---

Oryan Quest Busted/415 Gets Hit Again April 6, 1986

On Wednesday, April 2nd 1986, Oryan Quest was arrested on charges of computer invasion. Technically they only had him on one charge but later evidence accounted for the other two.

Oryan Quest was "busted" for hacking AT&T Mail, which is roughly similar to MCI
Mail. He had three different accounts, but the San Mateo Police and FBI only had suspicion of one. When they searched his home they found two more written down.

The charges against Oryan Quest were dropped for several reasons:

1. Illegal Search (they didn't have a warrant)
2. Police Brutality and Harassment (pushed him around and slammed his head into
   a car)

The authorities searched his house while Oryan Quest was at school, which is where they later arrested him.

What was taken includes the following:

Loads of computer disks
All printouts (his entire g-phile library)
10 Meg drive
Assorted Boxes (Blue, Red, Green, Silver)

His passwords, bbs numbers, codes, etc were undiscovered. (He believes)

No court date had been set as of yet, and it is believed that the prosecuting attorney will drop the case due to the earlier illegal proceedings by the SMPD.

Prior to his arrest the SMPD had been monitoring his line and had found that he
was scanning prefixes. This is however is inadmissible in a court of law because at the time that they were monitoring his line there was not sufficient
evidence for such action.

AT&T Mail was accessible through an 800 number, which Oryan Quest did call direct.

Some words from Oryan

"I have no intention of quitting hacking."

"My mistake was calling an 800 number direct and for fucking around with AT&T in the first place."

"I am more of a hacker than a phreak."

(Editor's note: When asked how he felt about what was happening he replied, "I'm not worried about it.")

Some other interesting facts about Oryan was that he held a part time job as a PacTel Operator. He, being 15 years old, had lied about his age (saying he was 16), but now has been fired.

Also SRI has given him a job offer for computer security. He is thinking about it but doesn't plan on accepting it.

Information provided by Oryan Quest through interview by Knight Lightning

---

Overlord 815 Arrested For Check Fraud

"The only reason I got caught was greed."

That was the Overlord (815)'s first statement to me during an interview on April 6, 1986. He says that originally, a long time ago, he concentrated on Western Union, but then later turned to credit card fraud. As he progressed, he learned that credit card fraud only worked about 5% of the time. He wanted something that worked 100% of the time. He found it...check fraud.

In his home town he acquired around $4,000 worth of equipment from 3 stores. Some of the merchandise consisted of an Apple //e (with every card possible, the best drives, monitors, etc...), a complete Commodore 128 system, and ten packs of disks for good measure. His downfall was going back to one of the same stores the next day to try it again.

He was instantly caught and tricked by the police to reveal more than he would have if he had really known his rights.

Check fraud is a felony crime. Although I myself am uninformed as to how to perform the art of check fraud, it must require a phone because Overlord (815) informs me that the police have labeled his crime as Telefelony. The actual charge however is for "theft by deception".

His home was not searched and he has given all the merchandise back.

He had told me that he plans to stop running his bulletin board Spectre III and sell his computer. This is mainly so he cannot be referred to as a computer hacker. IE: The prosecuting lawyer would ask, "Do you have a computer?!" He can truthfully say NO.

He plans to have the bbs run from the home of The Master (815) and the number would stay the same.

Another account of this story by TWCB Inc, says that Overlord has changed his mind and is not selling his computer or taking down Spectre III.

The court date is set at April 9, 1986, Overlord (815) says that the worst that
can happen is probation, a fine, civil service work, or any combination of the three.

Information provided by Overlord (815) during interview with Knight Lightning

---

TAP: Latest News From TWCB April 8, 1986

Well, as many of you may have noticed, TWCB Inc. did not fulfill their promise of having TAP Magazine out by April 7, 1986. When asked about this on that date, they replied that they had all the stuff, but it had to be typeset, formatted, printed, and distributed. They estimated that they could have it done in another four days. This secondary deadline was also not achieved.

The writers (according to TWCB) include:

Abbie Hoffman/Ace/Final Impulse/Gary Seven/Knight Lightning/Mark Tabas/Taran King/Susan Thunder/The Bootleg/The Cracker/The Firelord/The Metallian/TUC

The magazines supporting TAP include:

Mad Mad Magazine/High Times/Bootlegger Magazine/Hacker Magazine

Scan Man dropped himself from the TAP Staff.

By issue #6, TWCB plans to have a 112 page magazine. This is due to the fact that by then they plan to be receiving many more articles and will have several
more companies advertising.

The first issue of TAP Magazine will have articles on the following topics:

ISDN: Parts by Taran King and The Bootleg
Fiber Optics
Cellular Phones
Satellite Jamming
Moving Satellites
The Teltec Bust: Surfer Bill/The Firelord/TWCB Inc/Knight Lightning
Dr. Who Bust
History of TAP
RSTS 8.0
Signalling Systems: Taken from Phrack Inc. Newsletter
Introduction to PBXs: by Knight Lightning, taken from Phrack Inc. Newsletter
ROLM: By Monty Python, taken from Phrack Inc. Newsletter
MCI Overview: by Knight Lightning, taken from Phrack Inc. Newsletter
New BBS Laws: by Sally Ride, taken from Bootlegger Magazine
Cosmos: by Lex Luthor and the Legion of Hackers, taken from Bootlegger Magazine
Private Audience: by Final Impulse, taken from Phrack Inc. Newsletter
UNIX: by The Cracker
MAX Profile: by Phantom Phreaker, taken from Phrack Inc. Newsletter
Crashing Dec 10s: by The Mentor, taken from Phrack Inc. Newsletter
Pak Time: by Kerrang Khan
Techniques of Tracing
ESS: by Mark Tabas

Information provided by TWCB Inc. during interview with Knight Lightning

---

Quick Notes

On March 23, 1986, The Radio Station BBS in New York celebrated its one year anniversary. It now has one meg of storage online.

The rumor that Taran King was on a talk/news program in New York discussing hacking is completely wrong. Dead Lord started it, but as yet no one knows why.

The Tempest in 805 was burglarized in March. His computer and all other equipment among other things were stolen. This of course explains his absence from the bbs world for a while.

A reasonably new IBM kracking group, which was formally the Imperial Warlords, now known as Five-O, are re-kracking software and claiming it to be original by
themselves. Futhermore they are placing insulting messages inside the software towards certain individuals.

The Kidd of 408 got busted for busted for selling codes at his school for five dollars a piece. There was no particular company mentioned.

Video Stalker (408) carded some stuff to the home of Sinbad! Sinbad! told him that he would sign for the stuff, and when he did, he was arrested. No more details available.

The Tunnel, one of Austin, Texas's oldest phreak/hack boards, has come out of the closet. The Tunnel was revealed on the local news to be run by the computer crime division of the Austin Police Department. The two main goals of the board were to A) catch carders and B) catch Mentor and Cisban Evil Priest trying to sell those stolen computers. They were very successful at A.

Stronghold East elite has announced its new advisors. Hack Advisor: Lex Luthor
Phreak Advisor: Blue Buccaneer. The soon plan to have a name change due to the
fact that Apple Commander of Stronghold North insists they the two boards are affiliated while Slave Driver and Equalizer of Stronghold East feel differently. With instruction from Lex Luthor, SEE has enacted new security measures.

Thanx to 2600 Magazine, Stronghold East Elite now has the complete court transcripts of the bust that took place early last summer, most notably concerning Private Sector and 6 others, online for viewing.

Sigmund Fraud has been discharged as co-sysop of the Radio Station bbs.

-
Captain Crunch of 512 has stated that an auto-dial program that he wrote and uploaded was copied by TWCB Inc., who then claimed it as their own and signed their name in it.

_

==Phrack Inc.==

Volume One, Issue Five, Phile #12 of 12

=-=-=-

BBS, that one everyone now knows as the Catfur.
And Plovernet (305).

FL: Didn't you say that Teltec planted agents on all these boards?

SB: Yeah, that's what I was getting to. I don't know for a fact or anything but, what I hear is that Teltec employees posed as undercover hackers or phreakers and got on to the above listed boards. They had handles and infiltrated the system, having everyone believe that they were phreakers. Cause what they did was, well obviously they knew what they were talking about after all they worked for the company. They posted really educated information. From there I believe they actually posted some Teltec codes. There again, some of this is rumor, some of this is fact, I really couldn't tell you which was which.

FL: Well who all was busted?

SB: Jack Flack, Caeser D (John Kessler), Demetrius Cross, Dave Peters, several others of course. One whole family got busted, the father, the son, and the daughter. There is a list of thirty-eight people, their actual names were published in the Miami Review, which is a lawyer newspaper that goes to all the lawyers and judges in the Miami area. Another interesting thing is that the list mentioned a John Doe and a Jane Doe. There was a clause that said these two people are to be named at a later date, so who knows who that could be or even it was more than one person.

FL: You say Lex Luthor escaped?

SB: Yes he did.

FL: They were gonna snag him, but he escaped to California.

SB: I don't know exactly if they had him or whether they were gonna bust him or not but I know he was not mentioned.

FL: Maybe he was one of the John or Jane Doe people.

SB: Most of the stuff that I know is basically public information so I don't know anything about that John and Jane Doe stuff.

SB: An important point is that the Teltec agents posted some codes and then monitored those codes. I believe they cannot bust you for using those numbers because that's a form of entrapment. Instead what they'll do is monitor the calls, trace the calls, and then they will know who they are dealing with.

FL: They'll hook up a dialed number recorder (DNR) on the line.

SB: Well what this whole deal is doing is sorta pointing a finger of blame. Both people are wrong, Teltec is wrong in using entrapment to try and catch you, and you are wrong for using their codes to phreak. So what they do is keep an eye on you. So then they say "ah ha" this guy, John Doe over here is using this code. We know he has been abusing our system and now we are gonna keep an eye on him. So when this code goes dead, we're gonna watch and see if he uses any different ones and if he does, we'll bust him.

The main thing that's gonna come out of this court case is that they are gonna go after the the 5 people that were the system operators of the bbses. They're not really after the average user, what I think is happening is that the average users are going to be used as witnesses against the system operators.

The scary part about this case is that it is really pretty big because, it may set a precedent. If the judge rules in favor of Teltec and then Teltec presses charges, the subpoena says that there is a minimal of $5000 damage, and that's what they're seeking. So its gotta be well over $5000 damages. I tell you one thing, from the amount of money and information Teltec has put into this they are really determined to press charges. They invested a lot of money as far as lawyers and investigators. Another scary part of this story is that Teltec has not made the evidence that they have against the thirty-eight people public, as far as I know, and that's what everyone is afraid of. The average user doesn't know what he is up against.

FL: I bet the majority of the people on those boards are scared shitless now.

SB: Oh yeah, everybody is, its like the whole city of Miami is. Also I hear that Sprint and MCI will be cracking down in the future. They are most likely waiting to see how this case goes.

FL: Is Teltec the major service down there that everybody uses?

SB: Not really, it's one of many. The popular one these days is MCI cause it only has those 5 digit codes.

FL: I heard Teltec gave shitty connections.

SB: Yeah, that's funny because, I was talking to Jack Flack, and I said if you wanna crack up the people in the courtroom and you know that they are definitely gonna bust you, and that you're guilty beyond a shadow of a doubt, make a joke if they ask you what you know about Teltec say, "Alls I know about Teltec is that their connections to California are really shitty!" I don't know if they'd be too happy about hearing that one!

FL: So they are really gonna take care of this aren't they?

SB: Yeah but Teltec's main goal is to really get the system operators. You should read this subpoena here, it talks about the system operators. It says that the sysops "organized, financed, directed, and oversaw the illicit posting and trading of Teltec codes" "They failed to delete the messages containing illegal information." You see so the sysops are guilty cause they didn't delete the messages.

FL: The thing that could've solved all this is if people used random hackers and random destination numbers, like MegaPhreak.

SB: Another point is that even though you may be using a random hacker, most people aren't gonna be using the system at 3 a.m. to 4 a.m. The best time to scan is during normal business hours.

FL: That's true, after all you don't need 10,000 codes.

SB: Well anyway, I think that they are really after the system operators. And

if Teltec wins this case it will set a precedent. If all that happens then
I expect that we are gonna see a lot more of these cases popping up all around the country.

Editor's notes: There is some talk about there actually being 6 boards being busted and not just 5. Also the reference that Lex Luthor had any involvement or close calls with Teltec is only rumor. Other reports from 305ers who wish to remain un-named state that MCI has indeed stepped up its war on phreakers and hackers. Sysops, I really hope you watch who you let on.

Remember, a filter or fee for a bbs can easily be handled by agents or investigators. The best way to check on people is through references.

TWCB was also online during this interview, but as they gave little or no input to the actual content of this file all remarks from TWCB have been screened as they were worthless.

The original interview was done on a conference and recorded on cassette tape which was delivered to me. After which I wrote this file. This file was given permission to be printed in Phrack World News by The Firelord of 307 NPA.

- Knight Lightning

Telephone Testimony March 1986

Chairman Bill McGowan made a point to the House Subcommittee on Telecommunications. In testimony before the recently reconvened hearings on telephone industry competition, McGowan spoke against the "diversification frenzy" of the Bell Operating Companies (BOCs). He told the congressional subcommittee that the industry is still in the transition to full competition and cautioned against replacing a regulated monopoly with seven unregulated ones.

Information taken out of MCI World, March 1986 Issue

Kaptain Krash Busted

Kaptain Krash was caught stealing American Telephone & Telegraph's (AT&T) Teleconferencing time through an 800 PBX posted on P-80. He has been isolated from other members of the underground by his parents.

Note from Forest Ranger:

- LET THIS BE A LESSON TO THOSE WHO USE 800 PBX'S. 800 PBX'S ARE LIKE MAKING COLLECT CALLS AS TO WHERE YOUR NUMBER IS AUTOMATICALLY KNOWN. SO IT IS VERY EASY TO TRACE BACK TO YOU WHILE ON THE CONFERENCE OR A LATER CHECK WILL INDICATE THE SAME FINDINGS.

Information Provided By
F.R. Communications Newsline Service (c) 1986

_

Metal Shop Private Cleans House

On April 13, 1986, Taran King and Knight Lightning repurged the userlog deleting over 100 users from Metal Shop Private. This was mainly because of non-callers clogging up the log and to make sure there would be no extra accounts to lessen the security of the bbs.

People wishing to become members of Metal Shop Private, should contact Taran King or Knight Lightning via email. They then would be discussed with the Metal Shop Staff etc.

_

Dan Pasquale Seeks New Entertainment

This message is mainly for bbs sysops. Have you been receiving more calls from
people in the 415 NPA? In conversation with Dan Pasquale (See Phoenix Phortress Article in PWN III) High Evolutionary was told that Dan plans to try his hand at out of state bbses..."for fun." Let it be remembered that Dan Pasquale ran Phoenix Phortress BBS and as such saw posts for other phreak and hack bbses. Furthermore, as a bad habit, several bbsers seem to use the same passwords in more than one place. Therefore it is a possibility that Dan could
log on to bbses as someone else.

"The Radio Station Incident"

Oryan Quest had asked Broadway Hacker to remove him from the userlog for RS's own security. However BH decided not to do it at that time. Roughly a week later, someone using Oryan Quest's password logged onto the Radio Station BBS. This person was completely computer illiterate. Example: He typed "HELP" instead of "?" for a menu. When Broadway Hacker broke onto chat mode this Oryan Quest dropped carrier.

Please note: Although the police had to drop charges on Oryan Quest because of an illegal search this does not mean that the police couldn't have found his passwords.

Broadway also mentioned a rash of new users applying from 415 NPA.

Sysops beware.

Some Information Provided By
Broadway Hacker/High Evolutionary/Oryan Quest

_

Maxfield Speaks

In a Detroit newspaper, John Maxfield was interviewed by a reporter. Although I do not have the article or all the facts pertaining to it, it is known that the names mentioned include: Phantom Phreaker, High Evolutionary, Scan Man, Music Major, The Bootleg, and Slave Driver.

It is believed that Maxfield had acquired these names from P-80. However this is pure speculation.