UCRL-MA-119769

Department of Energy

C I A C

Computer Incident Advisory Capability

Accessing the CIAC Computer Security Archive

CIAC-2302 R.1

by the Members of the CIAC Team

January, 1995

Lawrence Livermore National Laboratory

Work performed under the auspices of the U. S. Department of Energy by Lawrence Livermore National Laboratory under Contract W-7405-Eng-48.

Table of Contents

Table of Contents, Continued

Introduction

What is CIAC?

CIAC is the U.S. Department of Energy's (DOE) Computer Incident Advisory Capability. Established in 1989—shortly after the Internet Worm—CIAC provides various computer security services free of charge to DOE's employees and contractors. CIAC services include:

- incident handling consulting
- computer security information
- onsite workshops
- white-hat audits

Overview

CIAC maintains an archive of computer security information for the DOE community. You can obtain documents and software in this archive through several access servers. This guide describes how to connect to these systems and obtain files from them.

This guide updates and replaces the previous CIAC-2302 guide entitled *The FELICIA Bulletin Board System and the IRBIS Anonymous FTP Server—Computer Security Information Sources for the DOE Community*.

CIAC Archive Contents

The CIAC archive contains a variety of useful information, including:

- publicly available CIAC, CERT, NIST, NASA, and DDN security bulletins
- virus descriptions, the VIRUS-L moderated virus news service and bulletin board, and copies of public domain and shareware virus-detection/protection software
- copies of useful public domain and shareware security-related utility programs
- Chris McDonald's computer security *Journal*
- *The Hack Report*
- reviews of anti-virus software and books by Slade and McDonald
- computer security conference announcements
- vendor descriptions of computer security software

Introduction, Continued

CIAC continually adds useful computer security information and software to the archive. CIAC welcomes any suggestions for additions to the archive.

The BBS Server

You can access the CIAC Bulletin Board System (BBS) via telephone with a modem. This system provides you with menus for selecting traditional BBS features. In the future, CIAC will make the BBS available over the Internet using Telnet.

The Anonymous FTP Server

Anonymous FTP access to the CIAC archive is available over the Internet at ciac.llnl.gov. To obtain information using the anonymous FTP server, you must have Internet access and be able to run FTP; E-mail access to the Internet is not sufficient. Using FTP, you can access the directory structure of the server. To locate files, you use the directories and 0-index.txt text files. Downloading information using the anonymous FTP server is much faster than using the BBS.

The World Wide Web Server

The most convenient access to the CIAC archive is the World Wide Web (WWW) server. A WWW client software such as NCSA Mosaic displays fully formatted hypertext documents on your screen to lead you to the information you need. Information often resides on another system. Using hypertext links, you can link to and display pages on other WWW servers by simply clicking on a word or phrase in an existing document. To use this feature, you need direct access to the Internet and a WWW client software such as Mosaic or Netscape.

NCSA Mosaic and Netscape are two distributed hypermedia browsers designed for information discovery and retrieval. These tools each provide a unified interface to the diverse protocols, data formats, and information archives used on the Internet. NCSA Mosaic is available by anonymous FTP from ftp.ncsa.uiuc.edu (141.142.20.50). Netscape's address is http://home.mcom.com/home/welcome.html.

Which Server to Use

If you have Internet access and want to browse through the information available, the WWW server is the most useful. If you have a specific file you need to download and know where it is located, the anonymous FTP server is the fastest. If you do not have access to the Internet, the BBS is your only option. If you want to join into DOE online discussions of security outside of the Internet newsgroups, use the CIAC BBS. Contact Bob Caldwell's office at DOE Headquarters in Germantown for a user ID.

Quick-Start Guide for Advanced Users

Using the CIAC Archive BBS Server

Getting Started

The CIAC archive BBS server is connected to the telephone system. To access the server with a modem and a terminal, set up your system as 8-bit, no parity, and one stop-bit. The access numbers are:

- (510) 423-4753—14.4K baud (V.32, V.42bis) and slower
- (510) 423-3331—9600 baud (V.32) and slower
- (510) 423-9885—19.2K baud ISDN within LLNL

When You Connect

The first time you call, you must register your name and address. Once you are registered, you can go directly to the file and message areas. To download or read files, switch to the file section and follow the instructions to download files. Most of the popular downloading protocols are supported, including XMODEM, YMODEM, SEALink, and KERMIT.

Scanning Downloaded Software

For any software you obtain, you should exercise caution and scan individual software before using it for the first time.

> ☞ **Unless otherwise indicated, all software in the CIAC archive has been scanned for known viruses. However, you should scan all downloaded software again with the most recent version of a virus-scanning tool.**

Be sure to scan archived applications after they have been extracted from the .ZIP, .ARC, or .SIT archive, as most scanning software cannot detect a virus in an application while it is still within an archive.

Shareware

If you are using a shareware package downloaded from the CIAC archive or from any other source, be sure to follow the instructions in the package for compensating the author. The cost is generally minimal ($10 to $50) for some very useful applications.

Using the CIAC Archive Anonymous FTP Server

Using FTP

The CIAC archive anonymous FTP server is available on the Internet. Type one of these commands to run FTP and connect to ciac.llnl.gov:

ftp ciac.llnl.gov

OR

ftp 128.115.19.53

When You Connect

Follow these steps to use the anonymous FTP server:

1. At the `Username:` prompt, type **anonymous**. If you do not see this prompt, type **user anonymous**.

2. At the `Password:` prompt, type your E-mail address (for example, **jdoe@llnl.gov**).

   All the computer security-related files and documents are in subdirectories of the directory "/pub/ciac".

4. To download files, use the "get" or "mget" command. The file "0-index.txt" in each directory lists the files in that directory and briefly describes their contents. The file "whatsnew.txt" in the "/pub/ciac" directory contains a list of the new files placed in the archive.

Using the CIAC Archive WWW Server

Using the WWW Server

To access the CIAC archive WWW server, use a Web client software such as NCSA Mosaic or Netscape.

Connecting to the WWW Server

Follow these steps to access CIAC archive information from the CIAC home page using Mosaic (the Netscape procedure is similar):

1. Start Mosaic and select **Open URL** on the **File** menu.
2. In the dialog box, type the URL address **http://ciac.llnl.gov/**.
3. When the home page opens, select **Add this Document** on the **Hotlist** menu to save the URL for rapid future access to the CIAC archive.

CIAC Archive User's Guide

Using the BBS Server

Getting Started

To access the BBS Server, you need a modem and either a terminal such as a VT100 or a Macintosh or PC running terminal emulation software. The best solution is a Macintosh or a PC running terminal emulation software; with this configuration, in addition to communicating with the BBS, you can download documents and software to your computer. Terminal emulation programs for the Macintosh include VersaTerm and VersaTerm Pro and shareware programs such as ZTerm or MicroPhone. For the PC, Qmodem is shareware, and Procomm is available in both shareware and commercial versions. The Windows 3.1 system includes a terminal emulation program.

Communi-cation Settings

The terminal or computer must be attached to a modem and the modem must be attached to the telephone network.

Set up the terminal or terminal software for 8 bits, no parity, 1 stop bit. Your terminal manual will describe how to do this. Most terminals have a setup feature where you can set these parameters.

You must also set the speed (known as the baud rate) at which information is sent to the modem. Common modem speeds are 110, 300, 1200, 2400, 9600, 14.4K, and 19.2K baud. The speed in characters-per-second is roughly the baud rate divided by 10, so 110 baud is about 11 characters, or about one word per second, while 1200 baud is about one line per second. The available speeds depend on your modem, the BBS modem, and the amount of "noise" on the telephone lines. You should generally use the highest speed compatible with both modems.

Most older modems operate at 1200 baud. Newer modems operate at 9600 baud, 14.4K baud, or faster, but they can operate at slower speeds if the foreign modem (the one at the other end of the telephone connection) cannot run that fast. With newer modems, set your terminal to communicate with your modem at the highest speed allowed. Your modem automatically negotiates the best speed with the foreign modem and slows down your transmissions (by buffering your input) to match. Newer modems also automatically compress and decompress data to increase the apparent speed.

BBS Modem Numbers

The CIAC BBS currently has two modems attached to it, plus ISDN service within LLNL. The CIAC BBS modem numbers are:

- (510) 423-4753—14.4K baud (V.32, V.42bis) and slower
- (510) 423-3331—9600 baud (V.32) and slower
- (510) 423-9885—19.2K baud ISDN access within LLNL

Line Speeds

CIAC BBS modems are capable of MNP data compression/decompression, so you may be able to get an apparent access rate well in excess of the rated speed if you have a compatible modem. If not, the modems can accommodate most slower modems and protocols.

The ISDN LLNL dataphone operates at high speed (19.2K baud).

Using a Hayes or Hayes-Compatible Modem

This section shows you how to install, test, and trouble-shoot a Hayes or Hayes-compatible modem.

Installing the Modem

If you have a terminal and a modem, the first step is to connect them together. You must have the right cable; different terminals and computers require different cables.

In this configuration, the modem is defined as a data set and the terminal as a data terminal. If you connect these two devices with a cable that has a male plug on one end and a female plug on the other, it should work.

You need to adjust your connections if you are using a computer as the terminal. Some computers are wired as a data set, and plugging a data set into a data set will prevent each device from functioning properly. In this case, you need a null modem (a double-ended connector) or a short cable with connectors on each end to switch some of the wires around to make a data set appear to be a data terminal.

If you do not understand RS-232, data sets, and data terminals, get help. Often the only way to determine whether a cable is correctly configured is to get a voltmeter and test each wire for its signals.

Testing Your Configuration

Follow these steps to test your Hayes or Hayes-compatible modem configuration:

1. Type **AT**, then press **<Enter>**. "AT" is the modem command for Attention and must precede all commands to the modem.

2. If the characters "OK" appear on the screen, then you are set up correctly.

Appendix A contains a list of some of the more common modem commands for Hayes and Hayes-compatible modems. Check your manual for appropriate commands for your modem.

Trouble-shooting

If your modem and terminal setup does not respond or prints the number "0", then it may have been configured to provide no response or to provide only brief responses. Follow these steps to reconfigure the setup:

1. To reset the modem, type **ATZ**, then press **<Enter>**. Type the string exactly as written, even if you do not see the characters on the screen while you type them. This is the reset command, and should turn echoing on and give text responses to commands.

2. Type **AT**, then press **<Enter>**. You should receive "OK" as a response. If your modem does not respond, or responds with garbage, check all your connections and the modem speed setting. If all seems well, then get knowledgeable help.

Modem connection and setup are still something of a black art.

Connecting to the BBS

The next step is to connect to the BBS. Use the modem to dial the telephone number listed earlier in this section that most closely matches the maximum speed of your modem. For example, if you are making a long-distance call on a Hayes-compatible modem to the first number on the list, type the dialing string **ATDT 15104234753.**

Most modems are Hayes-compatible; if yours is not, you will have to substitute your modem commands for the commands listed throughout these instructions.

> ☞ **If your telephone system requires special access numbers to get an outside line (e.g., "8" or "9"), include them as well, just as if you were dialing the number at a phone. You can also include parentheses, dashes, and spaces;most modems automatically format the dialing string internally. For example, the dialing string ATDT 1 (510) 423-4753 connects to the same number as ATDT 15104234753.**

When You Connect

After dialing the number, your modem and the BBS will communicate for a while and negotiate the best speed for communications. The response will usually be something like "CONNECT 9600". You are now connected to the BBS and should see the login screen.

Follow these steps if you do not see the login screen:

1. Press **<Enter>** twice. Try this once or twice, or until you see the login screen.
2. If you still do not see the login screen, possibly the BBS is down but the modem is still on. Hang up—use the "Hang-Up" command in the terminal emulator package or physically hang up the phone—and call again, or try the other BBS telephone number.
3. If you still do not receive a response, call CIAC for help.

Using a Non-Hayes-Compatible Modem

To use a non-Hayes-compatible modem, check your modem documentation for the appropriate commands to dial a number. Follow these steps to initialize dialing:

1. Most modems have a "Wake-Up" command. For example:

   press **<Enter>** or the **@** key twice

   OR

   press **<Enter>** twice, pause, then press **<Enter>** a third time.
2. Press the appropriate command key to dial the phone (usually **D**).
3. Press the appropriate command to set pulse or tone dialing (usually **P** and **T**), plus commands for any pauses you may need to get through a local PBX.

Logging On to the CIAC BBS Using a Hayes-Compatible Modem

Follow these steps to log on to the CIAC BBS using a Hayes-compatible modem. This example uses a 9600-baud connection.

1. Connect to your Hayes-compatible modem and type **ATDT94233331**. This string displays:

```
CONNECT 9600
```

   This screen then displays:

```
                  WARNING:  Unauthorized access to this
               computer system is prohibited.  Violators
              are subject to criminal and civil penalties.

                          WELCOME TO THE CIAC BBS

This BBS is run by the Computer Incident Advisory Capability (CIAC).
All users must register and truthfully answer the newuser questionnaire.

First Name?
```

2. Type your first name, then follow the prompts for your last name and your location. Press <**Return**> after each entry.

> ☞ **If this is your first logon, you will be asked to set your terminal type, supply a new password and answer the "New User Questionnaire." Follow the instructions on the screen. You will not see this on subsequent logons.**

The main menu displays:

```
CIAC BBS - Main Menu
Computer Incident Advisory Capability
=====================================

<W> - What's New On The CIAC BBS
<C> - CIAC Open Forum
<B> - Bulletins and System Notices
<A> - CIAC Advisories and Bulletins
<N> - CIAC Notes Journal
<2> - CIAC 2300 and other Security Documents
<F> - File Transfer Section
<H> - The Hack Report
<O> - Conference Bulletins
<D> - McDonald:  Information Systems Security
<J> - Bob Slade's Journal
<M> - Mail
<V> - Virus Database
<R> - Recent callers
<G>oodbye <T>ime <*>Utilities

Command:
```

3. Type the letter within the angle brackets to make your selection. The following table lists the menu selections and their contents.

Menu selection	Contents
<W>	Displays a bulletin containing the most recent additions to the BBS.
<C>	Switches to the CIAC Forum for open discussions among CIAC BBS users.
<B>	Contains some bulletins that describe CIAC and the role of this BBS.
<A>	Takes you directly to the CIAC download area to read or download CIAC advisories and information bulletins.
<N>	Takes you directly to the CIAC Notes download area to read or download the CIAC notes journal.
<2>	Takes you to the CIAC security document section to read or download CIAC 2300 series documents.
<F>	Takes you to the main menu of the file-transfer section. The file-transfer section contains CIAC and other notices, virus protection software, and other public-domain and shareware utilities.
<H>	Takes you to the Hack section to read or download *The Hack Report*, a listing of hacked and Trojaned software.
<O>	Takes you to the conference section for a list of notices for computer security related conferences.
<D>	Takes you to the McDonald section to read or download McDonald's journal.
<J>	Takes you to the Slade section to read or download Bob Slade's journal.
<M>	Opens the mail and dialog section. You can leave mail for other users, questions for the System Operator (SYSOP) of the BBS, or participate in the Dialog open forum.
<V>	Opens the virus database section. Here you can get information about different computer viruses and their characteristics.
<R>	Displays a list of recent callers.
<T>	Displays the amount of time you have been on the system. You are currently limited to 60 minutes a day. Leave a message for the SYSOP if you need more time.
<*>	Allows you to change your terminal type or password.
<G>	Asks you if you want to leave a message for the SYSOP, says good-by, and hangs up.

About Downloading Protocols

A downloading protocol is a method used to download a file and ensure it has downloaded correctly. The protocol you pick depends on the terminal you have and its capabilities. Most terminal emulators support XMODEM or KERMIT. While YMODEM and SuperKERMIT tend to be faster, pick the protocol you are most comfortable with. The TYPE protocol is only for short documents and simply prints the document on your terminal. For example, use TYPE to view a CIAC bulletin instead of downloading it to your computer. CIAC does not recommend using the ASCII download protocols. They are a last resort for systems that cannot use formal error-correcting protocols.

Obtaining Files From the CIAC BBS

Follow these steps to download files from the CIAC BBS:

1. At the BBS main menu, type **F**, then press <**Return**>.

   This menu displays:

```
CIAC BBS - File Transfer Section
Computer Incident Advisory Capability
==================================

<D> - Download Area
<U> - Upload Area
<O> - Outgoing
<->Previous Menu <G>oodbye <*>Utilities <T>ime

Command:
```

2. Type **D**, then press <**Return**>. This menu for the download section displays:

```
CIAC BBS - File Download Section
Computer Incident Advisory Capability
====================================

Select A Download Area From the Following List

<M> - Macintosh Files
<H> - Macintosh Utility Programs
<P> - PC files
<A> - Atari Files
<L> - CIAC 2300 and other Security Documents
<K> - The Hack Report
<C> - CIAC Documents
<I> - CIAC Notes
<E> - CERT Documents
<N> - NIST Documents
<D> - DDN Documents
<S> - NASCERT, NASA, SPAN Documents
<T> - ASSIST Documents
<V> - Virus-L Moderated News
<R> - Reviews of anti-virus software
<O> - Other useful stuff
-More-
<->Previous Menu <G>oodbye <*>Utilities <T>ime

Command:
```

3. Type the letter within the angle brackets, then press <**Return**> to make your selection.

> ☞ **At any time, press S to stop a listing or press P to pause.**

For example, type **P**, then press <**Return**> to select the next menu for PC files. This screen displays:

```
Type P to Pause, S to stop listing

PC-DOS/MS-DOS VIRUS DETECTION AND PROTECTION FILES

   The following files and programs are for PC and compatible computers
running PC-DOS or MS-DOS.
   Files with the .TXT extension are simple text files. They can be
downloaded with Xmodem, Ymodem or ASCII.
   Files with the .ZIP extension are .ZIP archives, and must be
extracted with PKUNZIP.EXE. PKUNZIP.EXE is in the file PKZ102.EXE, which
is a self extracting .ZIP archive. Download these with a binary protocol
such as Binary Xmodem or Binary Ymodem.
   Files with the .ARC extension are .ARC archives, and must be
extracted with ARC.EXE.
   Note that McAfee's software and Hoffman's virus Summary may not be
used by any organization without a license. However, they may be used by
individuals. Please read the license requirements in the documentation
supplied with the software before using it.

------------ New Stuff for PCs ------------
FP-214.ZIP 476162 9-26-94F-Prot antivirus v.2.14
TBAV624.ZIP       270210 9-26-94Thunderbyte antivirus v.6.24
VSUMX408.ZIP      845837 9-26-94Hoffman's Virus Summary 8/94

... Skipped Lines...


<D>ownload, <P>rotocol, <E>xamine, <N>ew, <H>elp, or <L>ist
Selection or <CR> to exit:
```

4. Type the letter within the angle brackets, then press <**Return**> to make your selection. The following table lists the menu selections and their contents.

Menu selection	**Contents**
<D>ownload	Download one or more files to your local machine.
<P>rotocol	Change the downloading protocol. The first time you download a file, this is done automatically (see step 5).
<E>xamine	View the contents in an ARC archive.
<N>ew	Followed with a date, lists files newer than that date.
<H>elp	Get help on these commands.
<L>ist	List this directory again.

5. Type **D**, then press <**Return**> to download a file. This prompt displays:

```
File Name?
```

6. Type the file name for your selection (e.g., **FP-214.ZIP**). The first time you download a file, the protocol menu displays:

```
Select from the following transfer protocols:

1 - TYPE file to your screen
2 - ASCII with DC2/DC4 Capture
3 - ASCII only, no Control Codes
4 - XMODEM
5 - YMODEM/YMODEM-g
6 - YMODEM/YMODEM- g Batch
7 - SEAlink
8 - KERMIT
9 - SuperKERMIT (Sliding Windows)

Choose one (Q to Quit):
```

7. Type the number for your selection, then press <**Return**>. This example shows the response for selecting the YMODEM/YMODEM-g Batch protocol for the file FP-214.ZIP:

```
Protocol=YMODEM  File FP-214.ZIP, 466 records
Est. Time:  10 mins, 26 secs at 192bps

Awaiting Start Signal
(Ctrl-X to abort)
```

Downloading to a Macintosh

When you are downloading to a Macintosh, be sure to set the correct version of the downloading protocol on your Macintosh. If you are downloading a text file, use the Text version of the downloading protocol (for example, Text-XMODEM, Text-YMODEM) on your Macintosh. The Text version of the downloading protocol corrects for differences in the end-of-line characters used on the PC and Macintosh systems—the PC needs a "CR-LF" at the end of a line, while the Macintosh needs "CR" only). When downloading a binary Macintosh file (e.g., a program file), a formatted document, or an archive, be sure to set the MacBinary form of the protocol (e.g., MacBinary-XMODEM) on your Macintosh. If you use the Binary instead of MacBinary protocol, you can do the conversion later, using either the Apple File Exchange utility included with the Macintosh system software or an archiving program, such as StuffIt from Aladdin Systems.

When you select the downloading protocol, the BBS pauses, waiting for you to enter a "start signal" at your terminal. Start your local download; if all goes well, your download will be complete in a few minutes.

Unpacking Compressed Archive Files

The methods for unpacking compressed files depend upon your configuration (PC-DOS/MS-DOS or Macintosh).

For PC Users

PC-DOS/MS-DOS files are either text files (.TXT), zip or arc archives (.ZIP or .ARC), or executables (.COM or .EXE). Text files and executables can be downloaded directly and used in their original form. Be sure to use a binary downloading capability such as XMODEM for the executable files and archives.

On the PC, the most common archive format is .ZIP. To extract files in the .ZIP format, you need either the PKUNZIP shareware utility or a DOS Shell program (e.g., Magellan) with a built-in .ZIP archive capability. For example, to extract all the files in the FP-204A.ZIP archive into the current directory, type, **pkunzip FP-204A.ZIP**.

If you type **pkunzip** without any arguments, the program will list the available command-line arguments for your selection.

Self-extracting archives are executable files (.EXE). Simply run the files and they will extract automatically.

For Macintosh Users

On the Macintosh, archived files are normally in StuffIt (.SIT) or Compactor/Extractor (.CPT) format. Run whichever program corresponds to the archive you want to extract. With the program running, open the archive file, select the files you want to extract, and select the Extract command (type **A** in StuffIt or select a menu item in Compactor). The files will be extracted to your disk.

SEA files are self-extracting archives. Simply run the files and they will extract automatically.

HQX files are BinHex files, a text format for a binary file. HQX files can be e-mailed. HQX files can be converted back to binary format using BinHex or Stuffit.

Using the Anonymous FTP Server

Access Requirements

The CIAC archive anonymous FTP server is available via the Internet at ciac.llnl.gov, IP address 128.115.19.53. To access files on the anonymous FTP server, you must have access to the Internet and must be able to run FTP on your computer. Your SYSOP will tell you if FTP is available and whether you are connected to the Internet.

Using FTP

Follow these steps to connect to the anonymous FTP server:

1. To open an FTP connection, type **ftp ciac.llnl.gov**

   OR

   If FTP is running, select the appropriate "Open" command, then type **ciac.llnl.gov** at the `ftp>` prompt

   OR

   If your computer cannot find ciac.llnl.gov, type the server Internet address **ftp 128.115.19.53**

   OR

   If FTP is running and your computer cannot find ciac.llnl.gov, type **128.115.19.53** at the `ftp>` prompt.

Trouble-shooting

If you cannot successfully connect to the server, contact your SYSOP.

When You Connect

Follow these steps to complete your login:

1. At the `Username:` prompt, type **anonymous**. If you do not see this prompt, type **user anonymous**.

Using the Anonymous FTP Server, Continued

2. At the `Password:` prompt, type your e-mail address (for example, **jdoe@llnl.gov**). Your password will be hidden. When you connect, this screen displays:

```
220 ciac FTP server (Version wu-2.4(6) Mon May 2 15:51:50 PDT 1994)
ready.
user anonymous
331 Guest login ok, send your complete e-mail address as password.
230-
230- This is the Ciac archive, provided and maintained by
230- the Computer Security Technology Center, Lawrence
230- Livermore National Laboratory.
230-
230- All activity is logged with your host name and email address
230-
230- If your FTP client crashes or hangs shortly after login, try
230- using a dash (-) as the first character of your password.
230-
230- Send comments/questions/problems to: ciac@llnl.gov
230-
230-
230 Guest login ok, access restrictions apply.
```

Locating Files

The following table lists the commands you can use to move through the directory system and download files:

Command	Action
cd	Change directory. Follow this command with the path to the directory you want to access. Use ".." as the directory name to return to the previous directory or "/" to return to the login directory.
ls	List the file and directory names within a directory.
dir	Full directory listing, including file size, modification dates, ownership, and permissions.
binary	Change the mode for downloading files to binary. Select this command before downloading any type of file except pure text files to ensure an unmodified file.
ascii	Change the mode for downloading to ASCII. If you have switched to binary mode, select this command before downloading pure text files. FTP automatically changes the end-of-line characters for your computer.
get	Get a file. Follow this command with the name of the file you want to download to your machine.
mget	Multiple get. Follow this command with a file name that includes wildcard characters to select and download multiple files. The wildcard character "*" stands for any number of any characters (including none), and "?" stands for any single character.
put	Upload a file to the server. This command is not allowed in most directories.
mput	Multiple put. Upload multiple files to the server. This command is not allowed in most directories.
close	Close the connection to the remote machine.
quit	Close any connections and end FTP.
?, h, help	List the available commands.

Contact your SYSOP for any additional commands you may require.

Listing Directories

The “ls” command lists all the files and directories in the current directory, for example:

```
ls
200 PORT command successful.
bin
usr
0-index.txt
dev
.login_message
incoming
pub
etc
150 Opening ASCII mode data connection for file list.
226 Transfer complete.
```

Changing Directories

The “cd” command followed by a directory name moves you to that directory. The “..” directory name always moves you to the parent directory of the current directory. This example shows a “cd” to the public (pub) directory, then lists the files in that directory:

```
cd pub
250 CWD command successful.
ls
200 PORT command successful.
spi
ciac
nid
150 Opening ASCII mode data connection for file list.
226 Transfer complete.
```

Accessing CIAC Files

This example shows how to change directories to the "ciac" directory and list its contents:

```
cd ciac
250 CWD command successful.
ls
200 PORT command successful.
ciacdocs
bulletin
notes
patches
whatsnew.txt
secdocs
sectools
util
150 Opening ASCII mode data connection for file list.
226 Transfer complete.
```

Contents of CIAC Files

The following table lists the CIAC files and their contents.

File name	Contents
ciacdocs	Directory: CIAC 2300 series computer security documents.
bulletin	Directory: CIAC Bulletins.
notes	Directory: CIAC Notes journal.
patches	Directory: Security patches.
whatsnew.txt	File: Text file of new additions to the server.
secdocs	Directory: Computer security documents from other response teams, including conference information, and software reviews.
sectools	Directory: Security-related software tools and anti-virus software.
util	Directory: Utility programs and archiving utilities.

Accessing CIAC Bulletins

This example shows how to change directories to the "bulletin" directory and list its contents:

```
cd bulletin
250 CWD command successful.
ls
200 PORT command successful.
fy89
a-fy90
b-fy91
c-fy92
d-fy93
e-fy94
f-fy95
xref.txt
150 Opening ASCII mode data connection for file list.
226 Transfer complete.
```

Contents of the Bulletin Directory

Each of the "bulletin" subdirectories contains the CIAC notices for a particular fiscal year. CIAC notices are numbered with a letter followed by a sequence number, where the letter "A" is used for fiscal year 1990, "B" for 1991, and so forth. The document "xref.txt" is a text file containing a cross-reference of CIAC notices, platforms, and problem type. Each directory contains a file named "0-index.txt" containing the name of each notice and its number.

Accessing Virus Information

This example shows how to change directories to the “pcvirus” directory by returning to the “ciac” directory. You can also use the one-step “cd” path command “../sectools/pcvirus.”

```
cd ..
250 CWD command successful.
ls
200 PORT command successful.
ciacdocs
.private
bulletin
notes
patches
whatsnew.txt
secdocs
sectools
util
150 Opening ASCII mode data connection for file list.
226 Transfer complete.
cd sectools
250 CWD command successful.
ls
200 PORT command successful.
macvirus
pcvirus
atarivir
150 Opening ASCII mode data connection for file list.
226 Transfer complete.cd pcvirus
250 CWD command successful.
ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
226 Transfer complete.
killmnk3.zip
seclog.exe
chkdate.zip
0-index.txt
21a10.zip
fp-211.zip
30a06.zip
clean113.zip
vsig9305.zip
vshl205.zip

... lines deleted ...
```

Downloading a Text File from the "pcvirus" Directory

The "pcvirus" directory files contain descriptions of PC computer viruses and copies of virus protection software. The file named "0-index.txt" contains a list of the files and their purpose. Download this file using the "get" command to review the directory files. This example shows how to download the "0-index.txt" file:

```
get 0-index.txt
200 PORT command successful.
150 Opening ASCII mode data connection for 0-index.txt (14184 bytes).
226 Transfer complete.
14184 bytes received.
```

The file is downloaded to your computer in default ASCII mode. The ASCII mode automatically changes the end-of-line characters in text files for your computer. You can read the file with any text editor.

Downloading a Binary File

To download a binary file, change to binary mode. Use the "get" command to copy the file to your computer. Use the "mget" command followed by a file name containing wildcard characters "*" or "?" to download multiple files, where "*" stands for any number of any characters (including none) and "?" stands for any single character. For example, "mget *.exe" would download copies of all of the executable files in the current directory.

This example shows how to download the binary file "FP-214.ZIP:"

```
binary
200 Type set to I.
get fp-214.zip
200 PORT command successful.
150 Opening BINARY mode data connection for fp-214.zip (476162 bytes).
226 Transfer complete.
476162 bytes received.
```

Closing FTP and Quitting the Session

Use the "close" command to close the connection. Use the "quit" command to close the connection and quit the session. You should receive a response:

```
quit
<Goodbye.
```

Remember, if you download and use shareware programs from this or any system, be sure to follow instructions for compensating the authors.

Using the WWW Server

Internet Access

The CIAC WWW server is available via the Internet at ciac.llnl.gov, IP address 128.115.19.53. To access files on the CIAC WWW server, you must have access to the Internet and must be able to run a Mosaic client software (or similar software such as Netscape) on your computer. This chapter highlights Mosaic for access procedures. Netscape instructions are available within the application once you have it running.

You can access all public CIAC archive materials—including CIAC documents, documents of other response teams, and anti-virus software and information—through the CIAC home page at URL http://ciac.llnl.gov/.

Mosaic Availability

NCSA Mosaic was developed and is available at no cost from the National Center for Supercomputing Applications at the University of Illinois in Urbana-Champaign. There are currently three versions of Mosaic available:

- NCSA Mosaic for the X-Window System
- NCSA Mosaic for the Apple Macintosh
- NCSA Mosaic for Microsoft Windows

Obtain the one that fits your local needs. The X-Window version is available as source code that should compile on any UNIX system.

Downloading Mosaic Using FTP

Downloading Mosaic from the NSCA anonymous FTP server is similar to downloading files from the CIAC anonymous FTP server. Follow these steps to download NCSA Mosaic:

1. To open an FTP connection, type **ftp ftp.ncsa.uiuc.edu**

   OR

   If FTP is running, select the appropriate **Open** command, then type **ftp.ncsa.uiuc.edu** at the `ftp>` prompt

2. If your computer cannot find ftp.ncsa.uiuc.edu, type the server Internet address **ftp 141.142.3.135**

   OR

   If FTP is running and your computer cannot find ftp.ncsa.uiuc.edu, type **O 141.142.3.135** at the `ftp>` prompt.

When You Connect

Follow these steps to complete your login:

1. At the `Username:` prompt, type **anonymous**. If you do not see this prompt, type **user anonymous**.

2. At the `Password:` prompt, type your e-mail address (for example, **jdoe@llnl.gov**). Your password will be hidden. When you connect, this screen displays:

```
Guest login ok, send your complete e-mail address as password.
Password:

Welcome to NCSA's new anonymous FTP server! I hope you find what you are
 looking for. If you have any technical problems with the server,
 please e-mail to FTPadmin@ncsa.uiuc.edu. For other questions regarding
 NCSA software tools, please e-mail softdev@ncsa.uiuc.edu.

The mail archive-server is fully operational. Requests go to
 archive-server@ncsa.uiuc.edu and send problem reports to
 archive-manager@ncsa.uiuc.edu

Note to HyperFTP users: If you log in, and cannot list directories
 other than the top-level ones, enter a - as the first character of your
 password (e-mail address).

If your FTP client has problems with receiving files from this server,
send
 a - as the first character of your password (e-mail address).
If you're FTP'ing from Delphi, please remember that the Delphi FTP
client
 requires you to enclose case-sensitive directory and file names in
double
 quote (") characters.

You are user # 138 of an allowed 140 users.

Please read the file README
 it was last modified on Wed Aug 24 11:35:25 1994 - 69 days ago
Please read the file README.FIRST
 it was last modified on Mon Aug 1 10:28:27 1994 - 92 days ago
Guest login ok, access restrictions apply.
```

3. Type **cd Mosaic** to change to the Mosaic directory.

4. Type **ls** to list the directory contents. This screen displays:

```
IDUNNO.NCSA.UIUC.EDU>cd Mosaic
<CWD command successful.
IDUNNO.NCSA.UIUC.EDU>ls
<Opening ASCII mode data connection for file list.
Mac
Windows
Unix
Contrib
Documents
Licensing
Papers
...
<Transfer complete.
```

The Mosaic directory contains subdirectories for the Macintosh, Windows, and UNIX versions of Mosaic.

5. Type **cd** followed by the appropriate subdirectory name to change to the subdirectory, then type **ls** to list the subdirectory contents. This example shows how to download the Macintosh version of Mosaic:

```
IDUNNO.NCSA.UIUC.EDU>cd Mac
<CWD command successful.
IDUNNO.NCSA.UIUC.EDU>ls
<Opening ASCII mode data connection for file list.
.index
Apple
.accountrc
FAQ
...
LocalHome.html
NCSAMosaicMac.103.sit.hqx
copyright
NCSAMosaic.1.0.3.README
QuickStart.Txt
GIFS
Documents
Helpers
NCSAMosaic200A8.README
Related
NCSAMosaic200A8.PPC.hqx
NCSAMosaic200A8.68k.hqx
<Transfer complete.
```

6. Select and download one of the current versions of NCSA Mosaic available for the Macintosh:

   - The version with the .PPC extension is for Power PCs.
   - The version with the .68k extension is for 68000-based Macintosh computers.

   This example shows how to download version 2.0.0A8.PPC using the "binary" command:

```
IDUNNO.NCSA.UIUC.EDU>binary
Type: Image, Structure: File, Mode: Stream
IDUNNO.NCSA.UIUC.EDU>get NCSAMosaic200A8.PPC.hqx
 To local file: ncsappc.hqx
<Opening BINARY mode data connection for NCSAMosaic200A8.PPC.hqx
(1434176 bytes)
.
<Transfer complete.
```

   The file NCSAPPC.HQX is now located on your computer.

7. Use BinHex or Stuffit to convert the file from a .HQX file to a self-extracting archive.

8. Run the self-extracting archive file to obtain the software.

9. Follow the instructions included with the software to install NCSA Mosaic.

Downloading Mosaic Using Mosaic

If you already have Mosaic on your machine, it can be used to obtain the latest version of the Mosaic software. Follow these steps to obtain the latest version of Mosaic:

1. Start Mosaic and connect to the Mosaic default home page at URL http://www.ncsa.uiuc.edu/SDG/Software/Mosaic/NCSAMosaicHome.html

   OR

   Select **Open URL** on the **File** menu to input the URL address and load the home page.

2. The Mosaic home page displays several hypertext links pointing to the latest software versions. Select the appropriate version and follow the instructions. The software will be automatically downloaded to your computer.

Connecting to CIAC

Follow these steps to connect to the CIAC home page:

1. With Mosaic running, select **Open URL** on the **File** menu. In the dialog box, type **http://ciac.llnl.gov/** (the CIAC home page URL).

   The CIAC home page will display.

Downloading CIAC Files Using Mosaic

Once you have connected to the CIAC WWW server, follow these steps to download CIAC files:

1. The CIAC home page displays several hypertext links that point to the information in the CIAC archive. Select the appropriate link. A second page will open with an index to the available files.

2. Select the files you want to download.

A Few Final Words

The CIAC computer security archive servers are supported by CIAC for the U.S. Department of Energy and its contractors. These information servers contain current computer security information and software for all computers, from desktop units through mainframes. Accessing this information is a relatively painless process once your system is correctly set up. Correct setup is especially important for modems and terminals, so get help if you are having problems.

Once your setup is complete, you can connect to one of the servers quickly. With FTP or Mosaic you can download files from ciac.llnl.gov in a few seconds with a single command. Downloading from the CIAC BBS is somewhat slower because the files must go over the telephone lines.

If you are experiencing difficulty or suspect there is a problem with one of the servers, please contact CIAC at (510) 422-8193 or send e-mail to ciac@llnl.gov.

Appendix A
Commands for Hayes and Hayes-Compatible Modems

The following table lists commands for Hayes and Hayes-compatible modems.

☞ **Always start a modem command line with the "AT" command.**

☞ **You can then stack several modem commands on one line, for example: "ATL1Q1V0" sends the commands L1, Q1, and V0 to the modem.**

Command	Action
AT	Attention (wakes up the modem).
D	Dial the following number.
T	Use tones to dial the number (use P here if your telephone system is pulse-dialing only).
,	Pause 2 seconds.
L1	Speaker volume low.
L2	Speaker volume medium (default).
L3	Speaker volume high.
M0	Speaker off.
M1	Speaker on until carrier detect (default).
M2	Speaker on always.
Q0	Send responses to commands (default).
Q1	Do not send responses.
V0	Send responses as numbers.
V1	Send responses in words (default).
W	Pause for a second dial tone. Use this to pause for an outside line. When you are using a local PBX that requires an initial number (e.g., "8" or "9") to get an outside line, use this command to set a pause for the outside-line dial tone before dialing your number.
Z	Reset the modem to the defaults.

Reader Comments

CIAC updates and enhances the documentation it produces. If you find errors in or have suggestions to improve this document, please fill out this form. Mail it to CIAC, Lawrence Livermore National Laboratory, P.O. Box 808, Mail Stop L-303, Livermore, CA, 94551-9900. Thank you.

List errors you find here. Please include page numbers.

_____

_____

_____

_____

_____

_____

_____

_____

List suggestions for improvement here.

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Optional:

Name _____ Phone _____

Department of Energy

CIAC

Computer Incident Advisory Capability

Technical Information Department • Lawrence Livermore National Laboratory
University of California • Livermore, California 94551