

Department of Energy

CIAC

Computer Incident Advisory Capability

Electronic Resources for Security Related Information

CIAC-2307 R.1

by Richard Feingold

December, 1994



REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 12/1/1994	3. REPORT TYPE AND DATES COVERED Report 12/1/1994	
4. TITLE AND SUBTITLE Electronic Resources for Security Related Information CIAC-2307 R.1			5. FUNDING NUMBERS	
6. AUTHOR(S) Richard Feingold				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Booz Allen & Hamilton 8283 Greensboro Drive McLean, VA 22102			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) DOE Computer Incident Advisory Capability			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; Distribution is unlimited			12b. DISTRIBUTION CODE A	
13. ABSTRACT (Maximum 200 Words) Information Technology (IT) security professionals are battling network attackers. Each of the professionals—from the operations level down to the assistant computer security officer, whether classified or unclassified, manager or user—must maintain their ability to recognize the threat and acquire the appropriate countermeasures. They must gain and maintain knowledge and ability to use the ever increasing resources—on parity with the attackers. This paper opens the door for the novice and enlarges the opening for the expert. It increases the reader’s threat awareness and enables effective and efficient use of the resources that attackers will certainly use against us. In short, cognizance of electronic resources is critical—they are the common ground of both information technology threats and countermeasures. The attackers use the resources with abundant facility; we must become at least as proficient. The remainder of this section sets the perspective of				
14. SUBJECT TERMS IATAC Collection, information security, network attacker,			15. NUMBER OF PAGES 77	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT UNLIMITED	

DISCLAIMER

This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor the University of California nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial products, process or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or the University of California. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or the University of California, and shall not be used for advertising or product endorsement purposes.

This report has been reproduced
directly from the best available copy.

Available to DOE and DOE contractors from the
Office of Scientific and Technical Information
P.O. Box 62, Oak Ridge, TN 37831
Prices available from (615) 576-8401, FTS 626-8401.

Available to the public from the
National Technical Information Service
U.S. Department of Commerce
5285 Port Royal Rd.
Springfield, VA 22161

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

- Incident Handling consulting
- Computer Security Information
- On-site Workshops

CIAC is located at Lawrence Livermore National Laboratory and is a part of its Computer Security Technology Center. CIAC is also a founding member of FIRST, the Forum of Incident Response and Security Teams, a global organization established to foster cooperation and coordination among computer security teams worldwide.

Reference to any specific commercial product does not necessarily constitute or imply its endorsement, recommendation or favoring by CIAC, the University of California, the United States Department of Energy, or the United States Government.

This is an informal report intended primarily for internal or limited external distribution. The opinions and conclusions stated are those of the author and may or may not be those of the 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

Abstract.....	1
Introduction.....	1
The Threats	2
Resources and Counter-measures	4
Anonymous ftp.....	7
Electronic Bulletin Board Services	9
Electronic Conferencing	9
List Servers/ Information Sources	10
Network Information.....	10
Reference Services	11
USEnet News.....	12
The DOE Automated Departmental Directives System (ADDS)..	13
The National Institute of Standards and Technology (NIST) Electronic Bulletin Board Services	13
The DOE Computer Incident Advisory Capability (CIAC) File Server and Electronic Bulletin Board System	13
The National Computer Security Center (NCSC).....	14

Appendix A	1
Glossary and Notation.....	1
Anonymous ftp Sites.....	4
BBSs	11
IRC (Internet Relay Chat) Conferencing	12
List Servers/Information Sources	13
Network Information	14
Reference Services.....	15
Remailers.....	21
USEnet News.....	22
Mail Help.....	23
ftp Help	24
List Server Commands	25
rn Help	30
CIAC Electronic Bulletin Board and ftp Summary Guide	32
DOCKMASTER Resource Guide.....	35
Mail Example.....	38
eff Anonymous ftp Example.....	39
rn Example	42
NIST Dial Up Electronic Bulletin Board System Example.....	44
CIAC Anonymous ftp Example.....	48
CIAC Electronic Bulletin Board System Example	51
References	55
 Appendix B	
Contacting CIAC.....	1

Electronic Resources for Security Related Information

Abstract

The quantity, quality, and availability of electronic resources is multiplying rapidly. Information Technology (IT) security professionals must make timely and effective use of these resources if they are to contain the growing threats of globally networked attackers. This paper outlines the threats, including recent examples, and then provides multi-level descriptions of the abundant resources available to the information technology security community. These descriptions are valuable to everyone from networking novices to sophisticated experts. While the information is useful for the entire security community, this paper pays particular attention to Department of Energy requirements.

Introduction

Information Technology (IT) security professionals are battling network attackers. Each of the professionals—from the operations level down to the assistant computer security officer, whether classified or unclassified, manager or user—must maintain their ability to recognize the threat and acquire the appropriate countermeasures. They must gain and maintain knowledge and ability to use the ever increasing resources—on parity with the attackers. This paper opens the door for the novice and enlarges the opening for the expert. It increases the reader's threat awareness and enables effective and efficient use of the resources that attackers will certainly use against us. In short, cognizance of electronic resources is critical—they are the common ground of both information technology threats and countermeasures. The attackers use the resources with abundant facility; we must become at least as proficient. The remainder of this section sets the perspective of the exposition that follows.

Over two decades ago, the futurist Marshall McLuan made the (since oft-quoted) observation that “the electronic interconnections will make the Earth a global village.” It was a brilliant metaphor and qualitatively predicted the electronic way of life for many of us. What is far more problematic is the quantitative impact of the electronic interconnections on what we do—specifically, ensuring secure networking and computation for our constituents.

Electronic Resources for Security Related Information, Continued

The network¹ is the product of a rapidly developing technology and the need to interconnect information resources. As a recent phenomenon without historical precedence and paradigm, it raises new challenges to our abilities to manage vast resources. Often, the incremental cost of obtaining valuable information is insignificant. A document available on the network is an inexhaustible supply of its own copies. Most users are not only in instantaneous contact with each other, but with each other's private and public databases and other online information.

It is estimated² that there are over three million nodes on the Internet—the network of networks that links a significant portion of the Earth's intellectual community. Each machine on the Internet has between one and many thousands of users and these machines are found just about anywhere on the planet. In principle, any user on any node can access or transfer information to or from any other node, use its resources, and even log in to it.³

To the novice, this myriad of actual and potential connections, this diversity of protocols, this spectrum of philosophies is an incomprehensible maze. Remarkably, with a little training and a modest amount of determination bolstered by need, the electronic world opens a new facility in communications as well as a vast store of information. To obtain a true perspective of its expanse and appreciation of its capabilities, one must *experience* the network.

The Threats

The average computer attacker⁴ is no more a technological genius than the average driver is a brilliant automotive engineer. The danger is not so much his⁵ native intelligence as his acquired knowledge, training, and facility with the network structures. Notwithstanding the legal, moral, ethical, and pragmatic issues, trying to reduce the free flow of questionable information on the network would be unmanageable at best, trying to eliminate it would be unimaginable. Our goal as security professionals is recognition and understanding of the threats.

Attackers gain both qualitative and quantitative advantages from their facility with the network. Qualitatively, they have access to extremely effective communications channels. The Internet Relay Chat (IRC) allows them to anonymously and openly discuss whatever they want at minimal (if any) cost, while simultaneously being able to (surreptitiously) exchange private correspondences of any kind. For example, someone creates an accurate and instantly updatable index of online cracking tools and then posts it on the network, making it (and unlimited copies) immediately available to the global cracking community.

¹ The network for the purpose of this discussion is a generic term signifying the many methods of electronic interconnections. The conceptual domain is sometimes referred to as “*cyberspace*.”

² Recent estimates by reliable sources; there is no way to know for certain.

³ In practice, of course, many of the nodes have some degree of security which prohibits some or all levels of arbitrary access.

⁴ This document's term for an electronic criminal; other, possibly more ambiguous terms are *hacker*, *intruder*, *cyberpunk*, *phreak*, and so on.

⁵ The masculine pronoun with neutral intent is used for rhetorical smoothness. I find *s/he*, *his/her*, *his* or *her* awkward and distracting.

Electronic Resources for Security Related Information, Continued

This also highlights the quantitative aspect of the attacker advantage. The amount of time individuals save by immediately taking advantage of each other's efforts is immeasurable. They often use free⁶ resources and appear to have abundant personal time. Attackers frequently use personal computers as well as computer accounts on obliging or compromised systems to search the network for vulnerabilities.

Examples

Early in 1994, the Internet experienced a continuing series of “sniffer” attacks. That is, attackers compromised host systems, installed software that monitored and recorded specific Local Area Network transactions that included host name/user name/password combinations. Some intruders evaded detection through the use of sophisticated Trojan software. It only took a one or a few talented individuals to create the software and techniques that were then used by many to compromise at the least hundreds of thousands⁷ of accounts.

A full time physicist and part time computer security expert discovered a significant security vulnerability. It was in a popular operating system on a popular workstation. He wrote a program to exploit the vulnerability, complete with detailed comments, and submitted it to the vendor of the workstation as well as reliable computer security groups. The vendor responded and eventually created a patch to fix the vulnerability. Ironically, the program fell into attacker hands—we still do not know how, and is widely being used to exploit unpatched workstations. Evidently, the attackers can circulate the program quicker than the security community can disseminate the countermeasures.

⁶ Clearly any resource has a cost; chances are the crackers are not paying. When the marginal costs are so low, there is no economical way of recovering them at the user level—they are absorbed as institutional overhead.

⁷ CERT estimate.

Electronic Resources for Security Related Information, Continued

The Electronic Frontier Foundation⁸, a non profit organization created to promote the free exchange of information on the network (among other things), provides a repository for “Computer Underground Digest” (CUD) publications. Literary merit notwithstanding, these (quasi) periodicals frequently contain significant attacker information, including detailed methodologies on defeating toll call controls (Phone Phreaking), a complete list of credit card prefixes, intimate information on computer and network vulnerabilities, and so on. To get a feel for the authors’ level of defiance and perversity, one publication has detailed and accurate instructions on the construction of a light bulb bomb; another on how to manufacture nitroglycerine. Recently, someone posted a comprehensive index to the CUD—a substantial time and labor saving compendium for attackers.

The IRC links attackers from everywhere; they can exchange information (figuratively) across the table or under the table—in real time. Recently, user name password pairs from newly compromised university computer systems were openly posted on the IRC channel #hack.

Resources and Counter-measures

We will discuss several major network resources; there are others that may be found in the references at the end of this document; and there are still others that may be discovered simply by browsing the network. At the introduction of each resource, we will offer suggestions of how the resource may be used to counter attackers and other possible adverse activities. Of course, any technology that makes you more efficient and effective will help achieve that goal.

There is no single expert on all network resources. There is no single up-to-date compendium. There is no single structure that governs or manages all resources. The network is both planned and unplanned—with formal, defacto, and sometimes incompatible standards. Its growth is both revolutionary and evolutionary. This document provides a high level view of a selected subset of resources and services, providing sufficient detail for the novice to get started and most sophisticated users to learn something new.

⁸ The EFF provides an open, uncensored service with significant value to the general community as well as information security professionals.

Electronic Resources for Security Related Information, Continued

Electronic mail (E-mail) delivers messages between physically distant points, often within minutes. File transfer copies information at hundreds or thousands (or greater) characters per second.⁹ The USEnet news group service provides an open electronic exchange of information in thousands of special interest groups. The IRC provides conferencing where special interest groups meet electronically to “chat” and exchange information.¹⁰ Electronic Bulletin Board Services (BBS) are a relatively mature and stable method of information exchange. Electronic list servers provide moderated and unmoderated collection and dissemination of contributor supplied information on specific topics. There are electronic reference services that allow a user to hierarchically search the entire spectrum of network resources for specific subjects or services. Finally, there is a network information provider.

For information technology security specialists, discovering that attackers routinely exploit these network resources is the first step. Appreciating their strategic and tactical value is the next. The third step is learning how to use them. Experienced IT specialists, even those unfamiliar with Unix, TCP/IP, and/or the Internet, will find that the network is a timely and powerful strategic asset; a remarkably effective system of communication requiring their serious attention.

The following sections introduce each of the resources mentioned above¹¹ (E-mail first, the remainder in alphabetical order). The best and most effective way to learn is by doing. Examples and help texts for ftp and rn appear in the appendices. This is a rapidly emerging suite of resources, where good, up to date documentation is scarce. Even the online documentation tends to age quickly—and is usually only updated as an afterthought.

⁹ The proposed National Information Infrastructure (NII) calls for transfer rates of gigabits/second.

¹⁰ The conceptual location of the “chat,” since it is physically distributed among terminals and computers, is an excellent example of “cyberspace.”

¹¹ It is assumed for pedagogic purposes that the reader is familiar with the commands or languages cited. The appendix has specific examples as well as help listings.

Electronic Resources for Security Related Information, Continued

Electronic Mail

Electronic mail (E-mail) is the network's answer to "telephone tag," the seemingly interminable exchange of "please return my call" messages without direct communications. E-mail allows an individual to consider and reply to each message in his or her own time. It also allows tracking, filing, and other computer aided manipulations. All computer incident handling teams use E-mail to distribute their bulletins and advisories and communicate with each other, and most of the technical community¹².

E-mail is the most popular form of electronic exchange. If a location has any network access at all, it will have E-mail. There are several addressing schemes; we will consider only the popular and common hierarchical Internet form:

`user@localhost.subdomain1...subdomainn.topdomain`

which reads *user* at *localhost* in *subdomain₁* in ... in *subdomain_n* in *topdomain*. For example:

`joe@bigboy.xyzlab.gov`

which is user *joe* on host *bigboy* in subdomain *xyzlab* in the *government* domain. Mail applications vary, but they usually have addressing to individuals or lists, carbon copies, subject field specification, replying, forwarding, and from and date information in the header. They may also have blind carbon copies, binary file attachment, and message ID, received, resent from, and reply to in the header.

The command¹³ to read mail is:

mail [-options]

The command to send mail is:

mail [-options] recipient_list

Help is available by typing ***man mail*** at the command prompt or ***?*** prompt from within mail.

¹² Various groups are addressing issues of confidentiality and integrity; there are interim solutions.

¹³ Commands are assumed to be UNIX unless otherwise specified.

Electronic Resources for Security Related Information, Continued

You may E-mail anonymously through services offered by willing volunteer sites, called “remailers.” One such remailer is located at nowhere@bsu-cs.bsu.edu, and is operated by Chael Hall. (A list of some other sites appears in the appendix.) It guarantees anonymity and is simple to use. To use this service, make sure that the first two lines of your message contain the following:

```
first line      ::  
second line    Request-Remailing-To: fergp@sytex.com
```

Modify any .sig or .mailsig files to suppress signature additions before sending the message. This would reveal your identity.

Anonymous ftp

Anonymous ftp is the network’s main library facilitator—either directly, or more recently serving as a partial basis for the reference services. It opens a remarkably cooperative, extremely low cost, timely, ever increasing, and loosely coupled store of valuable (and not so valuable) information. Not only is there abundant information directly relevant for information technology security specialists, but there is the potential to effectively share greater quantities. For example, all bulletins of the incident response teams, shareware, and freeware¹⁴ are readily available from multiple anonymous ftp sites. It is equally as important for the security specialist to keep abreast of the attacker information also available from anonymous ftp sites. Ironically, some of the sites provide both kinds of information in the spirit of a completely open network.

Anonymous ftp is a special instance of the TCP/IP file transfer protocol, requiring only a user name of “anonymous”—if allowed by the remote site. The password is by convention expected to be your Internet address and user name. Anonymous ftp sites are often library repositories. If the directory is not known beforehand, /pub is usually a good place to start and then you can search down hierarchically.

¹⁴ Shareware is software for which the author requests a nominal fee if the user is satisfied with the product. Freeware is software distributed without cost as a public service.

Electronic Resources for Security Related Information, Continued

To connect to the remote system targ.sub.dom, enter:

ftp targ.sub.dom

At the user name prompt, enter your Internet address. For example:

hero@good.guy.gov

You can now list the top level directory:

ls [-l]

With the -l option, lines that begin with the character “d” will be subdirectories. You can change directories by entering:

cd <directory name>

Print the current working directory:

pwd

Copy a file:

get <file name>

Send a file:

put <file name>

And terminate the session:

quit

Some systems provide introductory or “tidbit” information through the finger command; its format is:

finger @<remote host name>

or

finger <username>@<remote host name>

Electronic Resources for Security Related Information, Continued

Electronic Bulletin Board Services

Security specialists use electronic bulletin board services (BBSs) as an alternative or in conjunction with E-mail and anonymous ftp. They can “meet” and correspond with other specialists, obtain security bulletins and software, and learn of the latest threats and countermeasures. The CIAC bulletin board service is a good example.

Electronic bulletin board services are usually accessed through dial up telephone, data network (such as X.25), or occasionally by Internet. These services tend to be PC oriented and require a suitable terminal package. Workstations and timesharing systems with out-dialing capabilities may also be used. CIAC, NIST, and the NCSC (through DOCKMASTER) provide electronic bulletin board (among other) services.

Electronic Conferencing

Electronic conferencing is effectively exploited by the attacker community and other special interest groups. IT security use has been for the most part using it to passively learn about new threats. It is an effective means of immediate, value added communications between physically (and perhaps socially) separate individuals.

Electronic conferencing has been enhanced with the recent development of the Internet Relay Chat (IRC) software. Your local computer (PC, Macintosh, workstation, timesharing system) must obtain the (public domain) software from one of the anonymous ftp sites listed in the appendix, or from some other source. Assuming you have Internet access, you then connect to one of the listed regional servers—preferably the geographically closest. If your local machine does not have the client software, you can telnet to the site listed in the appendix to achieve IRC access. Once connected, you may then view and select channels on which to “chat.” To maintain anonymity, use a “handle” rather than your real name if you decide to listen into channel #hack. Also, the server will reveal your Internet location to anyone inquiring—unless you go through the telnet server.

Information flow on IRC tends to be sporadic and frequently flies off on tangents. You can however, initiate a session, invoke recording to disk, and leave it unattended. Other channel participants may notice this, object, and terminate your connections. As a countermeasure, participants have created ‘bots (for robots): script programs designed to appear like a real person listening and making comments. Finally, information may be surreptitiously exchanged between other members of the channel.

Electronic Resources for Security Related Information, Continued

List Servers/ Information Sources

List servers provide the security specialist with timely, topic specific information on narrowly defined subjects. Examples include viruses (Virus-L), means of safely connecting to the network (Firewalls), and the risks of computer and network systems (RISKS digest).

List servers are electronic mailing lists provided to (qualified) individuals. Moderated lists require that each message be reviewed by a moderator before being resent to the mailing list; on unmoderated lists, all submissions are automatically resent to everyone. Digests are moderated lists that combine all significant messages into periodic mailings. Unless otherwise indicated, you may subscribe to a list by sending an E-mail message to the subscription with the single line:

subscribe listname

in the text (not subject) portion of the message. The list will then be sent to the address from which you requested the subscription.

Network Information

The Network Information Center provides registration information for nodes on the Internet. It is frequently used to find a responsible system administrator for a host that may be attacking a location. Such information includes one or more names, addresses, telephone numbers, and electronic mail addresses.

Network information is provided by the Network Information Center at:

rs.internic.net

You may *telnet* to that address and you will be automatically logged in. The system will show you a help screen and you may then enter commands to get information on users and addresses. The principle command is:

whois domain

or

whois subdomain

You may obtain similar information concerning European hosts by telnetting to:

whois.ripe.net

Electronic Resources for Security Related Information, Continued

Reference Services

Reference services are emerging as value added facilities to search through the ever increasing quantities of information available through the Internet. They have the potential to do everything from locating a source of Macintosh anti-viral software to providing the weather report for a city that you're visiting tomorrow.

There are several information servers that allow you to browse the network.

- **"Archie"** is an information locator with which you locate anonymous ftp files. At last count, it could locate 150 gigabytes of information at over 1000 sites. There are a variety of ways to connect, the simplest being where you telnet to one of the server sites listed in the appendix and log in as "archie" (no password is required).
 - **"Gopher"** is an Internet resource locator. Its preferred access is through client software on a PC or workstation, but it can be accessed through telnet from a terminal.
 - The **"Wide Area Information Server"** (WAIS) is a text retrieval system freely available from Thinking Machines Corporation.
 - The **"World Wide Web"** (WWW or W3) provides for the global sharing of academic information. Its source is available through anonymous ftp from CERN. Its growth has exploded in the last year (1994).
 - **"Mosaic"** is a rapidly growing, popular "hypermedia" implementation of WWW. According to its creators, it is "an Internet-based global hypermedia browser that allows you to discover, retrieve, and display documents and data from all over the Internet." It appears to be emerging as a potential de facto standard. Mosaic has the added virtue that it can reference most other services, such as Gopher and ftp (see the appendix in this document).
 - **"Hytelnet"** is a library catalog reference service.
-

Electronic Resources for Security Related Information, Continued

USEnet News

USEnet news is the interactive news service of the network. The security specialist can selectively read postings on computer security, viruses, privacy issues, attacker methodologies (by the attackers), specific hardware and software, and so on. The specialist can correspond with the authors either privately or through the news service. USEnet is an excellent way of not only learning what's happening, but meeting contemporaries. As with any news source, one should independently verify the information.¹⁵

USEnet news (sometimes referred to as netnews) is selectively accessed through various news reader applications. The news groups are hierarchically defined; some major roots are listed in the appendix. The news reader application for the purposes this discussion is *rn*.

Netnews is a methodology for exchanging information on a common topic. Original articles are "postings" from individuals. Readers may then post replies to postings, replies to replies, and so on. This sequence started by the original posting is called a "thread." News reader applications allow you to "kill" (eliminate) a posting, thread, or news group. Conventionally, if replies contain the text of the referenced posting, it should be indented and/or preceded by a distinguishing character, usually >. Since replies can be nested, one frequently sees postings including various levels of indentation. As a matter of practicality and courtesy, subject lines should be clear and concise.

The "rn" news reader is run by entering:

rn

You will be asked if you want to subscribe to recently added news groups. When that query is finished, you will then be asked to read specific groups. You can answer **yes**, **no**, or **quit**, or you can enter a news group level command. For example, to read the news group "alt.security", type:

g alt.security

at any point. You will then be shown the chronologically oldest article.¹⁶ Note that all articles have sequential numbers. You can mark the article as read and go on by entering **k**. You can read the next article by entering **n**. You can save an article by typing **s**. You can get a list of all articles by entering **=**. There are other commands that allow you to navigate through a selected news group. You can get help by typing **h**. Note that you must first quit reading one news group before you can go to another. Once you are back at the selection level, there are many commands that allow you to navigate through that process. Finally, you can exit completely by typing **q** at the selection level.

¹⁵ Forgeries (known as "spoofing") are possible and do occur occasionally.

¹⁶ If you see a *--more--(x%)* prompt at the bottom of the screen and are unfamiliar with *more* protocol, note the following. Pressing the space bar advances one page and typing **q** quits reading that article. You may also type most other *rn* commands, for example **n** or **=**.

Electronic Resources for Security Related Information, Continued

The DOE Automated Departmental Directives System (ADDs)

The DOE Automated Departmental Directives System (ADDs) is a database of current DOE and Headquarters Orders, Notices, and Secretary of Energy Notices. It features menu-driven text search and retrieval and reports providing summaries of current and newly issued Directives. The recommended ADDs workstation is an IBM PC (or compatible) with communication software (the FTTERM File Transfer and Terminal Emulator Program is “strongly recommended”), dial out capabilities, a Hayes compatible or BISCAMP modem supporting V.22 or V.32 protocol or DPU in headquarters, and an attached printer. To register, submit DOE forms 1450.5 and 1450.5A to Chief, Human Resource Information Systems, U.S. Department of Energy, AD-123/F-109, Washington, DC 20585. For further information or questions, contact George Hofman at (301) 903-2870.

The National Institute of Standards and Technology (NIST) Electronic Bulletin Board Services

The National Institute of Standards and Technology (NIST) maintains four electronic bulletin board systems for information exchange:

- Computer security
- Data management activities and applications
- Open Systems Interconnections standards activities
- North American Integrated Services Digital Network (ISDN) Users’ Forum (NIUF)

The telephone numbers appear in the appendix of this document.

The DOE Computer Incident Advisory Capability (CIAC) File Server and Electronic Bulletin Board System

The DOE Computer Incident Advisory Capability (CIAC) provides an electronic bulletin board service as well as anonymous ftp. These are in addition to their bulletins and advisories, which are distributed electronically, in hard copy, and (if of immediate importance) by FAX to DOE sites. The BBS and ftp services contain similar information, where the BBS is for those without Internet access. They both feature CIAC and other response team bulletins, virus information, computer security related shareware, utilities, and so on. Access information to these services appears in the appendix of this document. Use of the BBS is menu driven and self explanatory. An example of access to ftp services appears in the appendix (note that the current name “CIAC.llnl.gov” will be changing to “ciac.llnl.gov” in the near future). A draft summary document for using both resources appears in the appendix. CIAC will be publishing user documentation for both services in the future. If you need further information or help, call the CIAC hotline at (510) 422-8193.

Electronic Resources for Security Related Information, Continued

The National Computer Security Center (NCSC) DOCKMASTER

DOCKMASTER is a (Multics-based) subscription service of the National Computer Security Center (NCSC), that they consider an “Information Security Showcase.” Its large repertoire of available services (its users manual is over one hundred pages) includes E-mail, electronic bulletin boards, and allows hands-on software evaluation. Its Evaluated Products List rates computers and computer security products. Users can access online documents (such as the *Orange Book*), participate in online discussions, and learn about computer security conferences. Users can connect to DOCKMASTER through MILNET (part of the Internet), TYMNET (a packet switching service), and local dial-in. A registration packet may be requested by writing to NCSC, Fort George G. Meade, MD 20755-6000—Attn: DOCKMASTER Accounts Administrator. Note that Federal employees are “User Type 3”, contractors are “User Type 6” and the project should be “Catwalk” unless you were specifically assigned another one. The resource guide for DOCKMASTER appears in the appendix of this document. Further information is available by calling (410) 850-4446—and they are very helpful.

Appendix A

Glossary and Notation

[Note: Unix commands are case sensitive.]

<u>Term</u>	<u>Description</u>
{ }	alternate choice for the preceding item
[]	containing optional command switches; also, part of file name syntax for some anonymous ftp servers
< >	containing descriptions of fields for commands, such as file names
*	wildcard character in file name specification
^	hold down control key while depressing character following the ^
...	recursive wildcard directory
anonymous ftp	ftp service not requiring a secret password
archie	Internet ftp file locator reference service
bbs	electronic bulletin board system
bold type	things that are particularly helpful to attackers/hackers
<i>bold italics</i>	user input in examples
'bots	(from robots) routines to simulate intelligent activity on an IRC channel
CIAC	(the DOE) Computer Incident Advisory Capability
.com	commercial organization Internet address domain
<CR>	carriage return—Return key pressed by user
cracker	term for computer criminal (<i>see also</i> , hacker)
CPSR	Computer Professionals for Social Responsibility
CUD	Computer Underground Digest
cyberspace	the conceptual location of electronic interconnections and communications
CERT	Computer Emergency Response Team
des	Data Encryption Standard
DNS	Domain Name Service—methodology/implementation for routing TCP/IP messages
.edu	educational institution Internet address domain
EFF	Electronic Frontier Foundation; organization advocating open information on the Internet (among other things)
faq	frequently asked questions
FCC	Federal Communications Commission
(F/C)	FTS and commercial telephone number
finger	Unix command to obtain user information at a local or remote host
FIRST	Forum of Incident Response and Security Teams
flame	posting critical and sometimes derogatory comments in reply to a posting
freeware	software freely distributed at no cost with owner maintaining all rights
ftp	file transfer protocol; used to send or receive files over the Internet
FTS	Federal Telephone System
fyi	for your information
gif	graphic file format used to exchange pictures

gopher

Internet resource locator

Glossary and Notation, Continued

<u>Term</u>	<u>Description</u>
.gov	government agency Internet address domain
hacker	ambiguous term for computer criminal (original hackers were tinkerers in the positive sense; <i>see also</i> , cracker)
handle	electronic pseudonym used for effect and/or to mask identity
HP	Hewlett-Packard
HTML	HyperText Markup Language – “mark up” language for Mosaic hypertext
HTTP	HyperText Transfer Protocol
HYTELNET	Internet library reference service
IITF	Information Infrastructure Task Force
<i>italics</i>	defined terms (in text)
IRC	Internet relay chat; enhanced multi-member electronic conversation
ISDN	integrated services digital network; voice, data, etc., on the same transmission media
ISS	Internet Security Scanner—a tool for checking vulnerabilities
IT	Information Technology—a blanket term for computer, network, information related activities
kerberos	DES-based encryption scheme—intuitively, a distributed security server
kill	(reading news) eliminate a posting, thread, or newsgroup
MD5	message digest algorithm for cryptographic checksums
.mil	military organization Internet address domain
MIME	Multipurpose Internet Mail Extensions
mirror	duplication of an ftp distribution site to share distribution overhead
NASIRC	NASA Automated Systems Incident Response Capability
NCSC	National Computer Security Center
.net	backbone networking organization Internet address domain
NFS	Network File System
NIC	Network Information Center; assigns/maintains Internet addresses
NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
.org	non-profit organization Internet address domain
OSI	Open Systems Interconnection (networking standards)
PCMCIA	Personal Computer Memory Card International Association
pem	privacy enhanced mail
pgp	pretty good privacy (enhanced mail)
phreaks	attackers who specialize in telephone systems (freaks with a “ph”)
posting	USEnet news article
/pub	top level directory usually reserved for public anonymous ftp documents
public domain	software released into the public domain, having no owner or use restrictions
remailer	a site that forwards mail anonymously, removing any identity
rfc	request for comment; technical information notes
ripem	riordan's Internet privacy enhanced mail
rn	Unix read news utility
SERT	Security Emergency Response Team (Australia)
sha	secure hash algorithm
shareware	low cost software, freely distributed with “voluntary” payment requested from satisfied users
sysop	system operator (especially BBS)
.tar	Unix file name suffix; Unix archive program format; use <i>tar -fx filename</i> to retrieve

Glossary and Notation, Continued

<u>Term</u>	<u>Description</u>
TCP/IP	transport Control Protocol/Internet Protocol; networking protocol originally for Unix and now most other operating systems as well; used for the Internet
telnet	remote terminal protocol; used to login to remote hosts on the Internet (primarily Unix)
thread	original posting and all subsequent replies to that posting
TIS	Trusted Information Systems—developers of pem
Unix	generic term for a number of similar operating systems originally developed by Bell Labs
URL	Uniform (sometimes Universal) Resource Locator: addresses for WWW/Mosaic
.Z	Unix file name suffix; compressed format for transmission; use <i>uncompress</i> to expand

Anonymous ftp Sites

Format:

ftp internet address:optional directory

Log in as **anonymous**, and enter **your username and E-mail address** when prompted for a password. Directories usually begin /pub unless otherwise specified. This is not a complete list. You can often find additional information by viewing the parent directories of listed specific subdirectories. Numeric addresses, when available, appear in parentheses.

internet address: optional directory

Description/Comment

ames.arc.nasa.gov:pub/SPACE	NASA information, images, etc.
apple.apple.com	Apple/Macintosh
aql.gatech.edu:/pub/eff/CUD (128.61.10.53)	CUD
aql.gatech.edu:/pub/security/iss	security utilities
archive.cis.ohio-state.edu	security software
arisia.xerox.com	message-digest software
arizona.edu	astronomy programs
arthur.cs.purdue.edu:/pub/pcert/tools/unix /netlog-1.02.tar.g	Unix security tools
arthur.cs.purdue.edu:/pub/reports /TR823.PS.Z	password information
ashley.cs.widener.edu:/pub/src/adm /shadow-3.1.4.tar.Z	password management
aql.gatech.edu	ISS
athena-dist.mit.edu	kerberos software
ba.com	Bell Atlantic
bcm.tmc.edu:/pcnfs/pcnfsd.92.11.05.tar.Z	Sun patches
beach.utmb.edu	anti-virus software backup site
bell.com	telecommunications information
black.ox.ac.uk (129.67.1.165) :/src/security	security information
boombox.micro.umn.edu:/pub/gopher	gopher reference service software
bruno.cs.colorado.edu	?
byrd.mu.wvnet.edu /pub/ejvc /EJVC.INDEX.FTP	Electronic Journal on Virtual Culture
cert.org:/pub/virus-l/docs	Virus-L documentation
cert.org:/pub/...	security information (e.g., COPS, npasswd)
coast.cs.purdue.edu	security tools archive
coast.cs.purdue.edu:/pub/aux	security archive
consultant.micro.umn.edu	electronic bookstore
coombs.anu.edu.au:/pub/irc	IRC information
crl.dec.com:/pub/DEC/ultrix-faq.txt	Ultrix faq
cs.bu.edu:/IRC/support	IRC
cs.bu.edu:/pub/listserv	list server software
cs.utah.edu:/pub	?
cs.uwp.edu:/pub/msdos/wp/passwp.zip	breaking WordPerfect encryption
csn.org	security, etc.

Anonymous ftp Sites, Continued

internet address: optional directory

Description/Comment

cpsr.org:/cpsr/clinton	white house documents
crvax.sri.com	RISKS digest
csrc.nist.gov:pub/... (129.6.54.11)	NIST BBS, security bulletins, first contacts
cv.vortex.com:/privacy	privacy forum archives
dartvax.dartmouth.edu:/pub/security	
/passwd+.tar.Z	password security (Unix)
dartmouth.edu	security software
decuac.dec.com:/pub/DEC/ultrix-faq.txt	Ultrix faq
dftnic.gsfc.nasa.gov:[.FILES.MAC]	
MACSECURE31.HQX{SIT}	anti-virus software
dg-rtp.rtp.dg.com(128.222.1.2)	Data General security patches
dhvx20.csudh.edu:/global_net	global network
drgate.dra.com:/pub/gpo	GPO BBS
ds.internic.net:pub/the-scientist	<i>The Scientist</i> (periodical)
edcom.edu	information technology news
eeecs.nwu.edu	security software
emx.utexas.edu	security software
etext.archive.umich.edu/pub/CuD/cud	
(141.211.164.18):	CUD
eugene.utmb.edu:/pub/pgp	pgp
eugene.utmb.edu:/pub/virus-software/pc{macintosh}	pgp
	anti-virus software
export.lcs.mit.edu	astronomy programs
fau43.informatik.uni-erlangen.de	IRC
first.org:/pub	security information
freebie.engin.umich.edu	IRC client/server software ftp site
ftp.acsu.buffalo.edu:/pub/IRC	IRC client/server software ftp site
ftp.apple.com:dts/mac/sys.soft/imaging	Apple utilities
ftp.bio.indiana.edu:/util/gopher	gopher software
ftp.bsdi.com	BSDI
ftp.census.gov:/pub	Census bureau
ftp.cert.org:/pub/tools	security tools
ftp.cic.net	Internet use instruction
ftp.cisco.com/pub	Cisco (Router/Firewall Vendor)
ftp.cni.org:/CNI/documents/farnet	
/stories-index	Coalition for Networked Information Internet
ftp.ccmall.com	Information
ftp.cco.caltech.edu:/pub/bjmccall	security upgrades
ftp.comlab.ox.ac.uk:/pub/Zforum	white house documents
ftp.cs.berkeley.edu:ucb/sendmail	Z specification language
ftp.cs.bul.nl	security software
ftp.cs.purdue.edu:/pub/spaf/...	foreign nodes
ftp.cs.purdue.edu:/pub/spaf/COAST	security tools
/Tripwire	
ftp.cs.ttu.edu:/pub/asciiart	Tripwire security software
ftp.cs.uwm.edu:pub/comp-privacy	ascii art
ftp.cs.widener.edu:/pub/zen/...	computer privacy information
	Zen and the Art of the Internet: A Beginner's Guide to the Internet

Anonymous ftp Sites, Continued

internet address: optional directory

ftp.cs.wisc.edu:/connectivity_table
 ftp.cwru.edu:/security/unix-security.ps
 ftp.delmarva.com:pub/security
 ftp.denet.dk:/pub/misc/cm200-UFC.tar.Z
 ftp.digital.com:/pub/Digital/info
ftp.ee.mu.oz.au:/pub/text/Cud/...
ftp.eff.org:/pub/CUD/... (192.88.144.4)
 ftp.eff.org:/pub/IRC/lumberjak.shar
 ftp.einet.net
 ftp.eit.com:/pub/web.guide/
 ftp.es.net:/pub/networking-info/earn
 /nettools.ps{txt}
 ftp.es.net:/pub/security
 ftp.etext.org:/Zines/InterText
 ftp.eunet.no:/pub/text/online.txt
 ftp.fcc.gov
 ftp.funet.fi:/pub/unix/mail/zmailer/
 ftp@ghost.dsi.unimi.it:/pub/crypt/sci.crypt
 ftp.greatcircle.com:pub/firewalls
 FTP.GreatCircle.COM:pub/archive
 /firewalls.Z
 ftp.gwu.edu:/pub/hoffman
 ftp.hep.net
 ftp.inoc.dl.nec.com:pub/security/...
 (143.101.112.3)
 ftp.informatik.uni-hamburg.de:/pub/virus
 /texts/security
 ftp.informatik.uni-hamburg.de:/pub/virus
 /texts/tests
 ftp.informatik.uni-hamburg.de:/pub/virus
 /texts/catalog/msdosvir.zip
 ftp.isoc.org/isoc/charts
 ftp.lm.com:pub/interpedia
 ftp.maristb.marist.edu
 ftp.ncsa.uiuc.edu
 ftp.ncsa.uiuc.edu:/Mosaic (141.142.20.50)
 ftp.nec.com:/pub/security/socks/cstc
 ftp.next.com /pub/NeXTanswers/Files
ftp.netsys.com
 ftp.nisc.sri.com:netinfo/interest-groups
 ftp.nisc.sri.com:pub/zone
 ftp.ntia.doc.gov
 ftp.oar.net:/pub/OARnet/doc/oarsec.PS.Z
 ftp.ox.ac.uk
 ftp.pica.army.mil
 ftp.pnl.gov in the directory:/pub/pnlinfo
 ftp.psy.uq.oz.au:/pub/DES
 ftp.qucis.queensu.ca:pub/dalamb/
 college-email

Description/Comment

international connectivity table
 Unix security
 firewalls information
 password cracker
 Digital Equipment Corporation
computer underground digest
computer underground digest, indices, etc.
 IRC
 gopher sources
 directory of Cyberspace resources

 Internet resource guides
 security information
 Intertext electronic periodical
 network information—shareware book
 FCC
 more secure mailer (than sendmail)
 cryptography
 firewalls information

 firewalls digest
 cryptography
 High Energy Physics

 computer security tools

 security documents

 virus archives

 MS-DOS virus information
 Internet statistics
 electronic encyclopedia
 white house documents
 NCSA telnet
 Mosaic/WWW software
 SOCKS
 NeXT patches and security alerts
computer underground publications
 mailing lists, security, etc.
 definitions of Internet zones
 National Information Infrastructure
 Internet security
 cryptography
 privacy issues
 gopher software
 des

 how to find E-mail addresses

Anonymous ftp Sites, Continued

internet address: optional directory

Description/Comment

ftp.rpi.edu	computer mediated communications
ftp.sco.com	SCO Unix patches
ftp.sei.cmu.edu: /pub/dvk/passwd.ps	password security
ftp.senate.gov	U.S. Senate
ftp.sert.edu.au:/security/sert/tools	tools from Australian SERT
ftp.sgi.com:/pub/sgi/IRIX	SGI patches
ftp.sti.nasa.gov	NASA information
ftp.sura.net:pub/nic	network guides and resources
ftp.tansu.com.au:/pub/docs/security	security documentation
ftp.telebit.com:/pub/nomad/...	network observations
ftp.temple.edu:pub/info/help-net	glossary of computer oriented abbreviations and acronyms
ftp.tis.com	pem
ftp.tis.com:pub/firewalls	Internet firewall toolkit and papers
ftp.ucsd.edu:hamradio/packet/tcpip/crypto (128.54.16.7)	des source
ftp.unl.edu:/pub/archie/clients	archie client software
ftp.unt.edu:/pub	computer and network security information
ftp.usask.ca:/pub/hytelnet/pc (128.233.3.11)	HYTELNET software
ftp.utdallas.edu:/pub/staff/billy/libguide (129.110.10.1)	Internet library guide
ftp.uu.net	dictionaries, astronomy programs
ftp.uu.net:/tmp/CUPindex	CUD index
ftp.uu.net:~ftp/systems/sun/sun-dist	sun patches
ftp.win.tue.nl	TCP security tools
ftp.win.tue.nl:/pub/security /tcp_wrappers_6.3.shar.Z	TCP wrappers
ftpserver.massey.ac.nz:/pcnfs.sun	sun patches
furmint.nectar.cs.cmu.edu/security	security
garbo.uwasa.fi:/pc/uttl/wppass2.zip	breaking WordPerfect encryption
gatekeeper.dec.com (16.1.0.2)	Third party software for DEC systems
gatekeeper.dec.com:pub/DEC/DECinfo /DECnews-EDU	DECNEWS electronic periodical
gatekeeper.dec.com:/pub/DEC/ultrix-faq.txt	Ultrix faq
gatekeeper.decwrl.com	
gate.demon.co.uk	pgp
ghost.dsi.unimi.it:/pub/crypt	cryptography
ghost.dsi.unimi.it:/pub/security/atp.tar.Z	anti-tampering program, etc.
gopher.uiuc.edu	electronic bookstore
gs80.sp.cs.cmu.edu:/usr/anon/public /space-tech	technical space information
hafnhaf.micro.umn.edu	"Electronic Government Information Service"
halcyon.com:/pub/mirror/CUD/... (202.135.191.2)	mirror of ftp.eff.org
hopf.math.nwu.edu:pub/gn/gn-0.6.tar.Z	gopher software (GN)
ibm1.cc.lehigh.edu	Virus-L archives
idlastro.gsfc.nasa.gov	astronomy library
ietf.cnri.reston.va.us:/oc/inet93	INET conference proceedings

Anonymous ftp Sites, Continued

internet address: optional directory

Description/Comment

iitf.doc.gov	NII
info.umd.edu	Univ. of Maryland information/programs
info.umd.edu:/info/Computers/PC/Unix /uuexe520.zip	virus survey
iraun1.ira.uka.de	security, IRC
CIAC.llnl.gov (128.115.19.60)	CIAC
iris1.ucis.dal.ca:pub/gif	Voyager, Hubble, etc. GIFs
iskut.ucs.ubc.ca:/pub/Internet-drafts /draft-rsads-rivest-md5-02.txt	MD5 description
jbcondat@attmail.com	Chaos digest - mail server
jerico.usc.edu:pub/gene/kk	cryptographic papers
julius.cs.qub.ac.uk:pub/SpaceDigestArchive	Space Digest
kampi.hut.fi	DES software
kidd.vet.purdue.edu:/pub/users/wam /docs/legal	computer security documents
mac.archive.umich.edu	Macintosh archives
mac.archive.umich.edu:/mac/util/encryption	Macintosh encryption
mcafee.com	anti-virus products
mrcnext.cso.uiuc.edu	project Gutenberg online text
mcsun.eu.net	windows security
more@hpcwire.ans.net	technical news stories
naic.nasa.gov/files/general_info /earn-resource-tool-guide.ps, earn-resource-tool-guide.txt	network resources
nasirc.nasa.gov	NASIRC archives
net.tamu.edu:pub/security/TAMU	Texas AMU security tools
net-dist.mit.edu:/pub/PGP	PGP
net-dist.mit.edu:/pub/TechMail-PEM	PEM
netlib@research.att.com	compilers
network.ucsd.edu:intertext (128.54.16.3)	electronic periodical
nevada.edu:/pub/liaison/govnmnt.zip	Government information on the Internet
nic.funet.fi	network information center, Finland
nic.merit.edu:documents/fyi	network guides and resources
nis.nsf.net:/documents/rfc/...	"requests for comments" standards
nnsf.nsf.net	Internet documents
nri.reston.va.us:/ietf	Internet Engineering Task Force
ns.ripe.net:earn/earn-resource-tool-guide.ps, earn-resource-tool-guide.txt	network resource guide
nysernet.org:pub/resources/guides	network guides and resources
oak.oakland.edu	large software repository
oak.oakland.edu:pub/msdos/virus	virus information
ocf.berkeley.edu:/pub/Library/poetry	poetry
otabbs.ota.gov	Office of Technology Assessment (U.S. Federal)
pc10868.pc.cc.cmu.edu	lists
pencil.cs.missouri.edu:/pub/crypt	pretty good privacy (enhanced mail)
photo1.si.edu	Smithsonian photos
pioneer.unm.edu:pub/info/beginner-info	space imagery data
pit-manager.mit.edu:/pub/usenet/...	faqs for the newsgroups
prep.ai.mit.edu	general including fax security

Anonymous ftp Sites, Continued

internet address: optional directory

prep.ai.mit.edu:/pub/gnu/fax-3.2.1.tar.Z
 princeton.edu:/pub/pgp20
 pubinfo.jpl.nasa.gov
 pyrite.rutgers.edu
 rascal.ics.utexas.edu:mac/virus-
 Research.att.com:dist/Internet_security
red.css.itd.umich.edu:/CUD/...
 rtfm.mit.edu
 rogue.llnl.gov
 ripem.msu.edu
 ripem.msu.edu:pub/crypt
 risc.ua.edu:/pub/ibm-anti-virus
 rpub.cl.msu.edu
 rsa.com:/pub/...
 rsa.com:/rsaref/dist/930105
 rtfm.mit.edu:/pub/usenet
 rutgers.edu
 s1.gov:/pub/socks.tar.Z
 s6k.boulder.ibm.com
 sc.tamu.edu:pub/security/TAMU
 sipb.mit.edu:/pub/diswww/diswww.tar.gz
 slopoke.mlb.semi.harris.com:/pub/IRC
 soda.berkeley.edu:/pub/cyberpunks
 soda.berkeley.edu:/pub/cyberpunks/pgp
 software.watson.ibm.com
 solbourne.solbourne.com
 src.doc.ic.ac.uk:/computing/comms/irc
 src.doc.ic.ac.uk:/public/sun/pc-nfs
 /pcnfsd.92.11.05.tar.Z
 src-aux.src.umd.edu
 sumex-aim.stanford.edu
 sumex-aim.stanford.edu:/info-mac/virus
 sunsite.unc.edu
 sunsite.unc.edu:/home3/wais
 /white-house-papers
 sunsolve1.sun.com:/pub/patches
 s1.gov
 techreports.larc.nasa.gov:pub/techreports
 /larc/92
 thumper.bellcore.com:/pub/skey
 thumper.bellcore.com:/pub/crypt
 Town.Hall.Org
 uiunix.ui.org
 una.hh.lib.umich.edu:/inetdirsstacks
 unma.unm.edu
 urvax.urich.edu:[MSDOS.ANTI-VIRUS]
 /info-mac/virusux1.cso.uiuc.edu:
 /pc/virus

Description/Comment

net fax software
 pretty good privacy (enhanced mail)
 JPL
 security mailing list
 anti-virus software
 papers on firewalls and break ins
mirror of ftp.eff.org
 computer security information
 DECnet security tools
 ripem programs
 encryption software
 anti-virus software
 RSAREF
 cryptography
 RIPEM, RSAREF
 USEnet faq archive
 Columbia University Appletalk
 Unix security
 IBM security fixes
 network security tools
 electronic conferencing source (Discuss)
 IRC client/server software ftp site
 remailer usage
 pgp
 IBM fixes
 Solbourne information (including security fixes)
 IRC information

 Sun patches
 Macintosh information/software
 Apple software
 anti-virus software
 linux fixes

 white house documents
 SUN patches
 security software

 NASA technical reports
 s/key one time password software
 cryptography
 Edgar—Securities and Exchange information
 Unix standards
 Internet resource guides
 ethics, policy, legislation

 anti-virus software

Anonymous ftp Sites, Continued

internet address: optional directory

Description/Comment

ucsd.edu:/hamradio/packet/tcpip/crypto /des.tar.Z	DES code
uunet.uu.net:comp.sources.misc /volume23/smiley/part01.Z	smiley sources
venera.isi.edu	DNS tools
vitruvius.cecer.army.mil	binary gifs
van-bc.wimsey.bc.ca:/pub/crypto/PGP-2.1	pgp
world.std.com:/OBS /The.Internet.Companion/	Internet documentation
wsmr-simtel20.army.mil	large software repository
wsmr-simtel20.army.mil:PD1: <MSDOS.TROJAN-PRO> {PD3:<MACINTOSH.VIRUS>}	anti-virus software
wuarchive.wustl.edu	largest software repository
wuarchive.wustl.edu.: /doc/misc/*	documentation
wuarchive.wustl.edu:ftp/usenet /comp.virus/*	unix security
wuarchive.wustl.edu:usenet /comp.sources.misc/volume23 /smiley/part01.Z	smiley sources

Finger Sources

These are usually electronic “tidbits” you may obtain by typing:

finger <sourcename>

For example, to obtain local Livermore, CA weather, type:

finger weather@icaen.llnl.gov

BBSs

<u>BBS</u>	<u>Access Methods</u>
cc:Mail BBS	(415) 691-0401
CIAC	(510) 423-4573 (1200/2400 baud); (510) 423-3331 (9600 baud)
U.S. Commerce Department Internet access	(202) 482-3870 (2400 baud); (202) 482-2167 (9600 baud) Telnet to "ebb.stat-usa"
Fedworld BBS, access to federal information services, versatile, complex	(703) 321-8020 (sys op (703) 487-4608))
IITF bulletin board Backup Internet access Questions	(202) 501-1920 (202) 482-1199 Telnet to "iitf.doc.gov" and log in as <i>gopher</i> (202) 482-1835; E-mail cfranz@ntia.doc.gov
NIST computer security Internet access	(301) 948-5717 (2400 baud or less); (301) 948-5140 (9600 baud) Telnet to "cs-bbs.ncsl.nist.gov" (129.6.54.30)
NIST data management activities and applications	(301) 948-2048 or (301) 948-2059 (2400 baud or less)
NIST open systems interconnection standards	(301) 869-8630 (2400 baud or less)
NIST North American Integrated Services Digital Network User's Forum	(301) 869-7281 (2400 baud or less)
The Privacy Rights Clearinghouse BBS	Direct access: (619) 260-4670 At the local prompt enter <i>c teetot</i> At the login prompt enter <i>privacy</i> Follow instructions for new users
Internet access	Telnet to "teetot.acusd.edu" and follow the above steps
Read the USEnet newsgroup "alt.bbs" for information about bulletin board services.	

IRC (Internet Relay Chat) Conferencing

<u>Location</u>	<u>Description</u>
#hack	attacker channel (there are many other channels, most legitimate)
bradenville.andrew.cmu.edu	telnet server
cc.nsysu.edu.tw	telnet server - login: IRC
chatsubo.nerce.gov:login bbs	telnet server
ircserver.itc.univie.ac.at 6668	telnet server
IRC.ibmpcug.co.uk 9999	telnet server
IRC.santafe.edu	telnet server - login: IRC
cs.bu.edu:/IRC/clients	IRC client/server software ftp site
ftp.acsu.buffalo.edu:/pub/IRC	IRC client/server software ftp site
freebie.engin.umich.edu	IRC client/server software ftp site
slopoke.mlb.semi.harris.com:/pub/IRC	IRC client/server software ftp site
(US)badger.ugcs.caltech.edu	IRC server site (US)
csd.bu.edu	IRC server site (East Coast US)
disuns2.epfl.ch	IRC server site (Switzerland)
IRC.caltech.edu	IRC server site (West Coast US)
munagin.ee.mu.oz.au	IRC server site (Australia)
nic.funet.fi	IRC server site (Finland)
penfold.ece.uiuc.edu	IRC server site (Midwest US)
sunsystem2.informatik.tu-muenchen.de	IRC server site (Germany)
ucsu.colorado.edu	IRC server site (US)
ug.cs.dal.ca	IRC server site (Canada)

List Servers/Information Sources

<u>List Server/Source</u>	<u>Description</u>
bugtraq-request@fc.net cert@cert.org cert@cert.org ciac-listproc@llnl.gov ciac-listproc@llnl.gov comp-privacy-request@pica.army.mil gopher-news-request@boombox. micro.umn.edu interpedia-request@telerama.lm.com isoc@nri.reston.va.us listproc@educum.edu listserv@itocsivm.csi.it LISTSERV@KENTVM.BITNET LISTSERV@LEHIGH.EDU LISTSERV@LEHIGH.EDU listserv@vmd.cso.uiuc.edu mac-security-request@eclectic.com Majordomo@GreatCircle.COM majordomo@is.internic.net Majordomo@Lists.EUnet.fi Majordomo@net.tamu.edu majordomo@nsmx.rutgers.edu pem-dev-request@tis.com pem-info@tis.com phrack@well.sf.ca.us privacy-request@cv.vortex.com risks-request@csl.sri.com security-alert@flatline.corp.sun.com security-features@sun.com tk0jut2@mvs.cso.niu.edu dds.hacktic.nl	bugtraq CERT - advisories CERT - tools CIAC - bulletin CIAC - notes computer privacy digest subscription gopher news subscription Interpedia online encyclopedia Internet Society News EDUCOM information technology news Network Information Retrieval and Online Public Access Catalogs HYTEL-L list sever (Internet library guide) MS-DOS viruses; <i>SUB VIRUS-L yourfullname</i> MS-DOS viruses alert; <i>SUB VALERT-L</i> <i>yourfullname</i> CUD, <i>SUB CUDIGEST YOUR NAME</i> Macintosh security subscription firewalls and firewalls-digest subscription scout-report, weekly happenings cryptography; SUBSCRIBE CYPHERWONKS academic-firewalls www-security pem subscription privacy enhanced mail information Phrack periodical privacy forum digest subscription risks digest subscription Sun security information Sun security alerts Computer Underground Digest (telnet) The Digital Cityt

Network Information

Telnet to “rs.internic.net”. The primary command is:

whois domain

or

whois subdomain

Reference Services

Archie

Archie is used for automated anonymous ftp server searches (see anonymous ftp for client software). There are multiple file locator sites (telnet to site and log in as **archie**):

archie.rutgers.edu (Rutgers University)
archie.unl.edu (University of Nebraska in Lincoln)
archie.sura.net (SURAnet archie server)
archie.ans.net (ANS archie server)

Gopher (Internet Resource Server)

- **Client software:**

boombox.micro.umn.edu:/pub/gopher
ftp.bio.indiana.edu:/util/gopher

- **Telnet access:**

consultant.micro.umn.edu (134.84.132.4)
gopher.uiuc.edu (128.174.33.160)
panda.uiowa.edu (128.255.40.201)

- **Servers:**

ace.esusda.gov – Americans Communicating Electronically (Department of Agriculture)
aclu.org – ACLU
ba.com – Bell Atlantic
bell.com – telecommunications information
csbh.com – Computer Solutions by Hawkinson
cix.org – commercial information
cwis.usc.edu – Gopher Jewels
dewey.lib.ncsu.edu – North Carolina State University Library
ds.internic.net – InterNIC network information service
educom.edu – EDUCOM Documents and News
fatty.law.cornell.edu – Cornell Law School
fedix.fie.com – Federal Info. Exchange (FEDIX)
gopher.acusd.edu – Privacy Rights Clearinghouse
gopher.bcm.tmc.edu – Baylor College of Medicine
gopher.census.gov – Census bureau
gopher.cic.net – Internet use instruction
gopher.cic.net:Electronic Serials/Alphabetic List/e/Electronic Journal on Virtual Culture/ – Electronic Journal on Virtual Culture
gopher.cni.org:70/11/cniftp/miscdocs/farnet – Coalition for Networked Information Internet Information
gopher.cpsr.org – CSPR
gopher.cs.ttu.edu – Texas Tech University
gopher.ed.gov – Department of Education
gopher.eff.org – EFF
gopher.epa.gov – EPA

Reference Services, Continued

gopher.es.net – Energy Sciences network
gopher.esa.doc.gov – U.S. Commerce Department
gopher.fcc.gov – FCC
gopher.first.org – FIRST
gopher.fonorola.net – Internet Business Journal archives
gopher.gsfc.nasa.gov – NASA Goddard Space Flight Center
gopher.house.gov – U.S. House of Representatives
gopher.Internet.com – Electronic Newsstand information
gopher.lanl.gov – Los Alamos National Laboratory
gopher.law.csuohio.edu – Cleveland State University Law Library
gopher.lib.umich.edu – University of Michigan Libraries, Internet
Resource Guides
gopher.nara.gov – National Archives
gopher.netsys.com (port 2100) – Electronic Newsstand (problems: E-mail
to staff@enews.com)
gopher.nist.gov – National Institute of Standards and Technology
gopher.ox.ac.uk:The World/Gopherspace/Alex – electronic texts
gopher.senate.gov – U.S. Senate
gopher-server.nist.gov – National Institute of Standards and Technology
(NIST)
gopher.sti.nasa.gov
gopher.tamu.edu – Texas A&M
gopher.tic.com – EFF-Austin/IMatrix Information and Directory Services,
Inc. (MIDS), Austin
gopher.town.hall.org – Internet radio
gopher.undp.org – United Nations
gopher.unr.edu – University of Nevada
gopher.vortex.com – Vortex Technology
gopher.well.sf.ca.us – Whole Earth 'Lectronic Magazine - The WELL's
Gopherspace
gopher.wired.com – public cryptography issues
hopf.math.nwu.edu – Internet Society, gopher software
ici.proper.com – Internet Computer Index
ietf.CNRI.Reston.Va.US
iitf.doc.gov – information infrastructure
info.asu.edu – electronic periodicals and educational gopher sites
info.learned.co.uk – LI NewsWire electronic periodical
internic.net – Network Information Center Gopher
jupiter.esd.ornl.gov – Oak Ridge National Laboratory ESD Gopher
krakatoa.jsc.nasa.gov – Library X at Johnson Space Center
lawnext.uchicago.edu – University of Chicago Law School
liberty.uc.wlu.edu – Washington & Lee University (Legal)
marketplace.com – Internet information mall
marvel.loc.gov – Library of Congress (LC MARVEL)
naic.nasa.gov – NASA Network Applications and Information Center
(NAIC)
ns.novell.com – Novell Netwire Archives
nsth.nsa.ca – electronic bookstore
ntiaunix1.ntia.doc.gov – National Information Infrastructure
ocs.dir.texas.gov – Department of Information Resources (State of Texas)
pdb.pdb.bnl.gov – Brookhaven National Laboratory Protein Data Bank
rs.internic.net – NIC

Reference Services, Continued

sluava.slu.edu – Saint Louis University (Legal)
SunSITE.unc.edu (152.2.22.81) – SUN information
technology.com – NASA Mid-Continent Technology Transfer Center
tic.com – Texas Internet Consulting
trainmat.ncl.ac.uk – network training
twinbrook.cis.uab.edu – Interpedia project
ucsbuxa.ucsb.edu (port 3001) – University of California - Santa Barbara
Library
una.hh.lib.umich.edu – University of Michigan Internet resource guides
vienna.hh.lib.umich.edu
vx740.gsfc.nasa.gov – NASA Shuttle Small Payloads Info
wired.com – writing
wiretap.spies.com – Wiretap
world.std.com – The World (Public Access Unix)

Wide Area Information Server

brewster@think.com – E-mail for further information
quake.think.com – telnet and sign on as “wais”
wais.eff.org – EFF

World Wide Web/Mosaic

- **Client software:**

info.cern.ch/pub/www/WWWLineModeDefaults.tar.Z - browser source
ftp.ncsa.uiuc.edu (141.142.20.50) – Mosaic

- **Servers (Uniform Resource Locators):**

You may access any anonymous ftp server xxx.yyy.zzz as ftp://xxx.yyy.zzz and any gopher server with the prefix gopher:// as illustrated below. The slashes (/) following the reference address delineate directory, subdirectory, ..., file name in the usual Unix notation.

gopher://aclu.org:6601/1 – ACLU
gopher://arl.cni.org:70/11/scomm/edir – directory of electronic journals
gopher://ba.com – Bell Atlantic
gopher://gopher.es.net/11/pub/security – Energy Sciences network
gopher://ntiaunix1.ntia.doc.gov:70/11s/newitems – National Information Infrastructure
gopher://oss968.ssa.gov – Social Security Administration
gopher://peg.cwis.uci.edu:7000/11/gopher.welcome/peg/GOPHERS/gov – U.S. Government
gopher://rsl.ox.ac.uk:70/11/lib-corn/hunter – electronic texts
gopher://una.hh.lib.umich.edu/11/inetdirs – University of Michigan
http://aps.org/ – American Physical Society
http://www.ba.com – Bell Atlantic
http://csrc.ncsl.nist.gov/ – FIRST
http://curia.ucc.ie/info/net/acronyms/acro.html – Acronym translator
http://delcano.mit.edu/ – NASA planetary data
http://delcano.mit.edu/cgi-bin/midr-query – NASA planetary data

Reference Services, Continued

<http://dfw.net/~aleph1> – cracker home page

<http://digicash.support.nl/> – digital cash

<http://ds.internic.net/ds/dsdirofdirs.html> – InterNIC network information center

<http://educom.edu/.index.html> – *EDUCOM*

<http://first.org> – FIRST

<http://ftp.etext.org/Zines/InterText/intertext.html> – electronic periodical

<http://http2.sils.umich.edu/~lou/chhome.html> or – University of Michigan

<http://ici.proper.com> – Internet Computer Index

<http://info.acm.org/> – ACM

<http://info.cern.ch/hypertext/DataSources/bySubject/Overview.html> – WWW virtual library

<http://info.cern.ch/wit> – WIT WWW conversation software

<http://info.cern.ch/hypertext/WWW/Clients.htm> – browser programs

<http://info.cern.ch/hypertext/WWW/FAQ/Bootstrap.html> – telnet accessible browsers

<http://info.cern.ch/hypertext/WWW/Shen/ref/shen.html> – Mosaic security

<http://info.isoc.org/interop-tokyo.html> – Internet information

<http://info.learned.co.uk> – *LI NewsWire* electronic periodical

<http://jupiter.esd.ornl.gov/> – Oak Ridge National Laboratory ESD

<http://lcweb.loc.gov/homepage/lchp.html> – Library of Congress

[http://login.eunet.no/\(presno/](http://login.eunet.no/(presno/) – Online World resources handbook

<http://marketplace.com> – Internet information mall

<http://nearnet.gnn.com/GNNhome.html> – Global Network Navigator

<http://pass.wayne.edu/business.html> – business on the Internet

<http://peterhe.ulib.albany.edu/mk-docs/mk-isp.html> – list of libraries

<http://power.globalnews.com/> – PowerPC News

<http://programs.interop.com>

<http://pubweb.parc.xerox.com/map> – Xerox PARC Map Viewer

<http://pubweb.ucdavis.edu/Documents/Quotations/homepage.html> – quotations

http://stardust.jpl.nasa.gov/pds_home.html – NASA planetary data

<http://sunsite.unc.edu/ianc/index.html> – “Underground music”

<http://web.nexor.co.uk/mak/doc/robots/robots.html> – WWW robots

<http://wombat.doc.ic.ac.uk/> – Online Dictionary of Computing

<http://www-ns.rutgers.edu/www-security/index.html> – WWW security

<http://www.anl.gov/oithome.html> – Department of Energy

<http://www.census.gov/> – Census bureau

<http://www.cis.ohio-state.edu/hypertext/faq/usenet/FAQ-list.html> – USEnet faqs

<http://www.charm.net/~web/Vlib.html> – WWW page development

http://www.commerce.net/directories/members/ns/new_ipower.html – National Semiconductor security products

http://www.cs.colorado.edu/homes/mcbryan/public_html/bb/summary.html – World-Wide WAIS-Searchable WWW Catalogs

<http://www.di.unipi.it/iconbrowser/icons.html> – Icon Browser at Pisa University

<http://www.digital.com/home.html> – Digital Equipment Corporation

<http://www.earn.net/lug/notice.html> – list servers

<http://www.ed.gov/> – Department of Education

<http://educom.edu/> – *EDUPAGE*

Reference Services, Continued

<http://www.ee.surrey.ac.uk/edupage/edupage/> – *EDUPAGE* electronic periodical
http://www.eecs.nwu.edu/hacker_crackdown/index.html – “The Hacker Crackdown”
<http://www.eff.org/ftp/EFF> – EFF
<http://www.eit.com/web/www.guide/> – guide to Cyberspace
<http://www.ensta.fr/Internet/> – Internet “goodies”
<http://www.fedworld.gov> – U.S. Government servers
<http://www.geom.umn.edu/docs/snell/chance/welcome.html> – probability and statistics
<http://www.hp.com> – HP Main Welcome Screen
<http://www.hpcc.gov/imp95/> – High Performance Computing and Communications
<http://www.hull.ac.uk/Hull/ITTI/itti.html> – United Kingdom's Information Technology Training Initiative
<http://www.ictp.trieste.it/Canessa/whoiswho.html> – Who's Who on the Internet
<http://www.ihep.ac.cn:3000/china.html> – Peoples Republic of China
<http://www.internic.net/> – the interNIC
<http://www.internic.net/infoguide.html> – guide to Internet WWW resources
<http://www.jou.ufl.edu/commres/webjou.html> – links to newspapers
<http://www.kiae.su/www/wtr/> – Window-to-Russia
<http://www.lib.umich.edu/chhome.html> or – University of Michigan
<http://www.lib.virginia.edu/etext/ETC.html> – University of Virginia
<http://www.llnl.gov> – Lawrence Livermore National Laboratory
<http://www.media.org/> – MIT security products
<http://www.mit.edu:8008/> – electronic conferencing (Discuss)
<http://www.nara.gov> – National Archives
<http://www.ncsa.uiuc.edu/SDG/Software/Mosaic/Docs/whats-new.html> – new server announcements
<http://www.netmarket.com/> – encrypted Mosaic
<http://www.openmarket.com/info/Internet-index/current.html> Internet tidbits
<http://www.ornl.gov/> – Oak Ridge National Laboratory
<http://www.research.att.com/> – ATT Bell Labs
<http://www.rpi.edu/~decemj/cmc/mag/current/toc.html> – Computer-Mediated Communication Magazine
<http://www.rpi.edu/Internet/Guides/decemj/text.html> – Internet resources
<http://www.scubed.com:8001/> – IRS and state tax forms
<http://www.sei.cmu.edu/FrontDoor.html> – Software Engineering Institute
<http://www.service.com/PAW/home.html> – Palo Alto Weekly
http://www.ssa.gov/SSA_Home.html – Social Security Administration
<http://www.tansu.com.au/Info/security.html> – security information
<http://www.tansu.com.au/hypermail/index.html> – mailing list archives
<http://www.tis.com/> – Trusted Information Systems
<http://www.town.hall.org/> – Internet radio
<http://www.tu-graz.ac.at/CHCIbib> – Human Computer Interaction
<http://www.utirc.utoronto.ca:3232/HTMLdocs/NewHTML/intro.html> – HTML documentation
<http://uu-gna.mit.edu:8001/uu-gna/text/index.html> – texts for online classes
<http://www.wais.com> – Wide Area Information Server
<http://www.wais.com/wais-dbs/risks-digest.html> – risks digest

Reference Services, Continued

<http://www.willamette.edu/~tjones/Spanish> – Spanish lessons

<http://www.wired.com> – public cryptography issues

<http://www.wsg.hp.com/> – HP Workstation Systems Group

<http://wwwhost.cc.utexas.edu/world/instruction/index.html> – instructional uses of the web

<http://130.20.92.130:8001/esh/home2.htm> – DOE Office of Environment, Safety and Health

Remailers

Edited List	1	hh@pmantis.berkeley.edu
	2	hh@cicada.berkeley.edu
	3	hh@soda.berkeley.edu
	4	nowhere@bsu-cs.bsu.edu
	5	remail@tamsun.tamu.edu
	6	remail@tamaix.tamu.edu
	7	ebrandt@jarthur.claremont.edu
	8	hal@alumni.caltech.edu
	9	remailer@rebma.mn.org
	10	elee7h5@rosebud.ee.uh.edu
	11	phantom@mead.u.washington.edu
	12	hfinney@shell.portal.com
	13	remailer@utter.dis.org
	14	00x@uclink.berkeley.edu
	15	remail@extropia.wimsey.com

Notes:

- 1 through 6: do not support encrypted headers.
- 7 through 12: support encrypted headers.
- 9, 13, 15: introduce longer than average delay; privately owned machines.
- 14: public key not yet released.
- 15: header and message must be encrypted together.

Others	admin@anon.penet.fi
---------------	---------------------

USEnet News

Relevant Major Roots	alt	alternative, testing
	comp	computer related
	gnu	software from Free Software Foundation
	ieee	IEEE related
	misc	miscellaneous
	sci	science
	talk	discussion of specific topic
	vmsnet	VMS related

Relevant Groups	austin.eff
	alt.bbs.lists
	alt.irc
	alt.privacy
	alt.security
	alt.security.index
	alt.security.pgp
	bit.listserv.infonets
	bit.listserv.virus-l
	comp.infosystems.gopher
	comp.org.eff.talk
	comp.risks
	comp.security.announce
	comp.security.misc
	comp.society.cu-digest
	comp.society.privacy
	comp.sources.binaries
	comp.sys.novell
	comp.virus
	misc.security
	sci.crypt
	sci.virus

Mail Help

Type ? at the mail prompt to display a help listing.

cd [directory]	chdir to directory or home if none given
d [message list]	delete messages
e [message list]	edit messages
f [message list]	show from lines of messages
h	print out active message headers
m [user list]	mail to specific users
n	go to and type next message
p [message list]	print messages
pre [message list]	make messages go back to system mailbox
q	quit, saving unresolved messages in mbox
r [message list]	reply to sender (only) of messages
R [message list]	reply to sender and all recipients of messages
s [message list] file	append messages to file
t [message list]	type messages (same as print)
top [message list]	show top lines of messages
u [message list]	undelete messages
v [message list]	edit messages with display editor
w [message list] file	append messages to file, without from line
x	quit, do not change system mailbox
z [-]	display next [previous] page of headers
!	shell escape

A [message list] consists of integers, ranges of integers, or user names separated by spaces. If omitted, mail uses the current message.

ftp Help

To display help about ftp, type *man ftp* at the Unix prompt.

Use these commands at the ftp> prompt:

append	append to a file
bye	terminate ftp session and exit
cd	change remote working directory
close	terminate ftp session
delete	delete remote file
dir	list contents of remote directory
disconnect	terminate ftp session
help	print local help information
get	receive file
lcd	change local working directory
ls	nlist contents of remote directory
mdelete	delete multiple files
mdir	list contents of multiple remote directories
mget	get multiple files
mkdir	make directory on the remote machine
mls	nlist contents of multiple remote directories
mode	set file transfer mode
mput	send multiple files
open	connect to remote tftp
put	send one file
pwd	print working directory on remote machine
status	show current status
user	send new user information

List Server Commands

Commands are listed in alphabetical order, with the minimum acceptable abbreviation in capital letters. Angle brackets are used to indicate optional parameters. All commands which return a file accept an optional "F=fformat" keyword (without the quotes) that lets you select the format in which you want the file sent; the default format is normally appropriate in all cases. Some esoteric, historical or seldom-used commands and options have been omitted.

List Subscription Commands (from most to least important)

SUBscribe listname <full_name> Subscribe to a list, or change your name if already subscribed

SIGNOFF Remove yourself:
listname - From the specified list
* - From all lists on that server
* NETWIDE - From all lists in the network

SET listname options Alter your subscription options:
ACK/NOACK/MSGack - Acknowledgments for postings
CONCEAL/NOCONCEAL - Hide yourself from REVIEW
Files/NOFiles - Toggle receipt of non-mail files from the list
Mail/NOMail - Toggle receipt of mail
DIGests/INDEX - Ask for digests or message indexes rather than
 getting messages as they are posted
REPro/NOREPro - Copy of your own postings?
TOPICS: ALL - Select topics you are subscribed to
 <+/->topicname (add/remove one or replace entire list)

Options For Mail Headers of Incoming Postings (Choose One)

FULLhdr or FULLBsmtp - "Full" mail headers
IETFhdr - Internet-style headers
SHORThdr or SHORTBsmtp - Short (default) headers
DUALhdr - Dual headers, useful with PC or Mac mail programs

CONFIRM listname1 <listname2 <...>> Confirm your subscription (when LISTSERV requests it)

Other List-Related Commands

INDEX listname Sends a directory of available archive files for the list, ifcpostings are archived

List Server Commands, Continued

Lists	<option> (no option) Detailed Global Global /xyz SUMmary <node> SUMmary ALL SUMmary TOTAL	Send a list of lists as follows: - Local lists only, one line per list - Local lists, full information returned in a file - All known lists, one line per list, sent as a (large!) file - Only those whose name or title contains "xyz" - Membership summary for all lists on specified node - For all nodes (long output, send request via mail!) - Just the total for all nodes
Query	listname *	Query your subscription options for a particular list (use the SET command to change them) - Query all lists you are subscribed to on that server
REGister	full_name OFF	Tell your name to LISTSERV, so that you don't have to specify it on subsequent SUBSCRIBE's Make LISTSERV forget your name
REView	listname <options> BY sort_field Country Name NODEid Userid BY (field1 field2) Countries LOCal Msg NOHeader Short	Get information about a list - Sort list in a certain order: - by country of origin - by name (last, then first) - by nodeid - by userid - You can specify more than one sort field if enclosed in parentheses: BY (NODE NAME) - Synonym of BY COUNTRY - Don't forward request to peers - Send reply via interactive messages (BITNET users only) - Don't send list header - Don't list subscribers
STats	listname <options> LOCal	Get statistics about a list - Don't forward to peers

Informational Commands

Help		Obtain a list of commands
Info	<topic>	Order a LISTSERV manual, or get a list of available ones (if no topic was specified)
Query	File fn ft <filelist> <options> FLags	Get date/time of last update of a file, and GET/PUT file access code - Get additional technical data (useful when reporting problems to experts)
RELEASE		Find out who maintains the server and the version of the software and network data files

List Server Commands, Continued

SHOW	<function>	Display information as follows:
	ALIAS node1 <node2 <...>>	- BITNET nodeid to Internet hostname mapping
	BITEARN	- Statistics about the BITEARN NODES file
	DISTribute	- Statistics about DISTRIBUTE
	DPATHs node1 <node2 <...>>	- DISTRIBUTE path from that server to specified node(s)
	DPATHs *	- Full DISTRIBUTE path tree
	FIXes	- List of fixes installed on that server
	LINKs node1 <node2 <...>>	- Network links at the BITNET node(s) in question
	NADs node1 <node2 <...>>	- Addresses LISTSERV recognizes as node administrators
	NETwork	- Statistics about the network
	NODEntry node1 <node2 <...>>	- BITEARN NODES entry for the specified node(s)
	NODEntry node1 /abc*/xyz	- Just the “:xyz.” tag and all tags whose name starts with “abc”
	PATHs snode node1 <node2 <...>>	- BITNET path between “snode” and the specified node(s)
	STATs	- Usage statistics (default option)
	(no function)	- Same as SHOW STATS

Commands Related to File Server Functions

AFD		Automatic File Distribution
	ADD fn ft <filelist <prolog>>	Add file or generic entry to your AFD list
	DELete fn ft <filelist>	Delete file(s) from your AFD list (wildcards are supported)
	List	Displays your AFD list
	For node administrators: FOR user ADD/DEL/LIST etc	Perform requested function on behalf of a user you have control over (wildcards are supported for DEL and LIST)
FUI		File Update Information: same syntax as AFD, except that FUI ADD accepts no “prolog text”
GET	fn ft <filelist> <options> PROLOGtext xxxx	Order the specified file or package - Specify a “prolog text” to be inserted on top of the file
GIVE	fn ft <filelist> <TO> user	Sends a file to someone else
INDex	<filelist>	Same as GET xxxx FILELIST (default is LISTSERV FILELIST)
PW	function	Define/change a “personal password” for protecting AFD/FUI subscriptions, authenticating PUT commands, and so on
	ADD firstpw	- Define a password for the first time
	CHange newpw PW=oldpw	- Change password
	DELete oldpw	- Delete password

List Server Commands, Continued

SENDme Same as GET

Other (Advanced) Commands

DATAbase function	Access LISTSERV database:
Search DD=ddname	
<ECHO=NO>	
List	- Perform database search (see INFO DATABASE for more information on this)
REFRESH dbname	- Get a list of databases available from that server
	- Refresh database index, if suitably privileged
DBase	Same as DATABASE
DISTRIBUTE <type> <source> <dest> <options>	Distribute a file or a mail message to a list of users (see INFO DIST for more details on the syntax)
Type:	
MAIL	- Data is a mail message, and recipients are defined by "<dest>"
FILE	- Data is not mail, recipients are defined by "<dest>"
RFC822	- Data is mail and recipients are defined by the RFC822 "To:" / "cc:" fields
Source:	
DD=ddname	- Name of DDname holding the data to distribute (default: "DD=DATA")
Dest:	
<TO> user1 <user2 <...>>	- List of recipients
<TO> DD=ddname	- One recipient per line
Options for the general user:	
ACK=NOne/MAIL/MSG	- Acknowledgement level (default: ACK=NONE)
CANON=YES	- "TO" list in "canonical" form (uid1 node1 uid2 node2...)
DEBUG=YES	- Do not actually perform the distribution; returns debug path information
INFORM=MAIL	- Send file delivery message to recipients via mail
TRACE=YES	- Same as DEBUG=YES, but file is actually distributed
Options requiring privileges:	
FROM=user	- File originator
FROM=DD=ddname	- One line: "address name"
FOR user command	Execute a command on behalf of another user (for node administrators)
SERVE user	Restore service to a disabled user
THANKs	Check if the server is alive
UDD	Access the User Directory Database (there are 18 functions and many sub-functions, so the syntax is not given here)

List Server Commands, Continued

Syntax of Parameters

filelist	= 1 to 8 characters from the following set: A-Z 0-9 \$#@+_-:
fformat	= Netdata, Card, Disk, Punch, LPunch, UUencode, XXencode, VMSdump, MIME/text, MIME/Appl, Mail
fn	= same syntax as "filelist"
ft	= same syntax as "filelist"
full_name	= firstname <middle_initial> surname (*not* your E-mail address)
listname	= name of an existing list
node	= BITNET nodeid or Internet hostname of a BITNET machine which has taken care of supplying a "Internet." tag in its BITEARN NODES entry
pw	= 1 to 8 characters from the set: A-Z 0-9 \$#@_-?! %
user	= Any valid RFC822 network address not longer than 80 characters; if omitted, the "hostname" part defaults to that of the command originator

rn Help

To display help about rn, type **man rn** at the Unix prompt

Use these commands at the Newsgroup Selection command level:

y, SP	Do this newsgroup now.
.cmd	Do this newsgroup, executing cmd as first command.
=	Start this newsgroup, but list subjects before reading articles.
u	Unsubscribe from this newsgroup.
c	Catch up (mark this newsgroup all read).
n	Go to the next newsgroup with unread news.
N	Go to the next newsgroup.
p	Go to the previous newsgroup with unread news.
P	Go to the previous newsgroup.
-	Go to the previously displayed newsgroup.
1	Go to the first newsgroup.
^	Go to the first newsgroup with unread news.
\$	Go to the last newsgroup.
g name	Go to the named newsgroup. Subscribe to new newsgroups this way too.
/pat	Search forward for newsgroup matching pattern.
?pat	Search backward for newsgroup matching pattern. (Use * and ? style patterns.)
l pat	Append r to include read newsgroups.)
l pat	List unsubscribed newsgroups containing pattern.
m name	Move named newsgroup elsewhere (no name moves current newsgroup).
o pat	Only display newsgroups matching pattern. Omit pattern to unrestricted.
a pat	Like o, but also scans for unsubscribed newsgroups matching pattern.
L	List current .newsrsrc.
&	Print current command line switch settings.
&switch {switch}	
	Set (or unset) more command-line switches.
&&	Print current macro definitions.
&&def	Define a new macro.
!cmd	Shell escape.
q	Quit rn.
x	Quit, restoring .newsrsrc to its state at startup of rn.
^K	Edit the global KILL file. Use commands like /pattern/j to suppress pattern in every newsgroup.
v	Print version.

Use these commands at the Article Selection command level:

n, SP	Scan forward for next unread article.
N	Go to next article.
^N	Scan forward for next unread article with same subject.
p, P, ^P	Same as n, N, ^N, only going backward.
-	Go to previously displayed article number.
number	Go to specified article.

rn Help, Continued

range{,range}:command{:command}	Apply one or more commands to one or more ranges of articles. Ranges are of the form: number number-number. You may use "." for the current article, and "\$" for the last article. Valid commands are: e, j, m, M, s, S, and .
/pattern/modifiers	Scan forward for article containing pattern in the subject line. (Use ?pat? to scan backwards; append "h" to scan headers, "a" to scan entire articles, "r" to scan read articles, "c" to make case sensitive.)
/pattern/modifiers:command{:command}	Apply one or more commands to the set of articles matching pattern. Use a K modifier to save entire command to the KILL file for this newsgroup. Commands "m" and "M", if first, imply an "r" modifier. Valid commands are the same as for the range command.
f, F	Submit a followup article (F = include this article).
r, R	Reply through net mail (R = include this article).
e dir{command}	Extract to directory using /bin/sh, uuencode, or specified command.
s ...	Save to file or pipe via sh.
S ...	Save via preferred shell.
w, W	Like s and S but save without the header.
...	Same as s ...
C	Cancel this article, if yours.
^R, v	Restart article (v=verbose).
^X	Restart article, rot13 mode.
c	Catch up (mark all articles as read).
b	Back up one page.
^L	Refresh the screen. You can get back to the pager with this.
X	Refresh screen in rot13 mode.
^	Go to first unread article. Disables subject search mode.
\$	Go to end of newsgroup. Disables subject search mode.
#	Print last article number.
&	Print current values of command line switches.
&switch {switch}	Set or unset more switches.
&&	Print current macro definitions.
&&def	Define a new macro.
j	Junk this article (mark it read). Stays at end of article.
m	Mark article as still unread.
M	Mark article as still unread upon exiting newsgroup or Y command.
Y	Yank back articles marked temporarily read via M.
k	Kill current subject (mark articles as read).
K	Mark current subject as read, and save command in KILL file.
^K	Edit local KILL file (the one for this newsgroup).
=	List subjects of unread articles.
u	Unsubscribe from this newsgroup.
q	Quit this newsgroup for now.
Q	Quit newsgroup, staying at current newsgroup.

CIAC Electronic Bulletin Board and ftp Summary Guide

The following information was provided by the guide's author. Note that the name of the anonymous ftp server will be changing to "CIAC" at a later date.

The FELICIA Virus Bulletin Board System and the CIAC Anonymous FTP Server Computer Security Information Sources for the DOE Community—Executive Summary

by
William J. Orvis

The Computer Incident Advisory Capability (CIAC) operates two file servers for the DOE community, FELICIA (formerly FELIX), and CIAC. FELICIA, is a computer Bulletin Board System (BBS) which is available via telephone using a modem. CIAC is an anonymous FTP server on the Internet. Both of these file servers contain all of the publicly available CIAC, CERT, NIST, and DDN bulletins, virus descriptions, the Virus-L moderated virus bulletin board, copies of public domain and shareware virus detection/protection software, and copies of useful public domain and shareware utility programs.

ACCESSING FELICIA

FELICIA is a BBS connected to the telephone system. To access it with a modem and a terminal, set up your system as 8 bit, no parity, and one stop bit. The access numbers (commercial and FTS) are:

(510) 423-4753 - 2400 baud or slower
(510) 423-3331 - 9600 baud V.32 or slower

The first time you call in, you will have to register your name and address. To download or read files, switch to the file section and follow the directions. Most of the popular downloading protocols are available, including XMODEM, YMODEM, SEALink, and Kermit.

ACCESSING CIAC

CIAC is an anonymous FTP server on the Internet, so you must have Internet access to use it. Note that CIAC.llnl.gov will change to ciac.llnl.gov in the near future. Use one of the following commands to run FTP with CIAC' Internet address:

ftp CIAC.llnl.gov
or
ftp 128.115.19.53

When you are connected to CIAC, if you get the username prompt, type **anonymous**; otherwise, type **user anonymous**.

when you are asked for a password, type your E-mail address (e.g., jones@llnl.gov.)

There is a document explaining the directory of downloadable files stored in the file 0-index.txt in the first level directory. All the computer security-related files and documents are in subdirectories of the directory /pub/ciac.

CIAC Electronic Bulletin Board and ftp Summary Guide, Continued

To download files, use the GET or MGET command (see below). The file 0-index.txt in each directory lists the other files in that directory and briefly describes their contents. The file news.txt in the /pub/ciac directory contains a list of the new files placed in the archive.

Use the following commands to move around the directory system and download files:

- cd Change directory, follow with the path to the directory you want to access. Use “..” as the directory name to backup one directory or “/” to backup to the root directory.
- ls List the contents of a directory.
- binary Change the mode for downloading files to binary. Execute this command before downloading anything but pure text files, to insure that you get an unmodified file.
- ascii Change the mode for downloading to ASCII. If you have switched to binary mode, execute this command before downloading pure text files. FTP automatically changes the end of line characters to the ones your machine expects.
- 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, and “?” stands for any single character.

SCANNING DOWNLOADED SOFTWARE

As with any software you obtain, you should exercise caution and scan individual software packages before using the software for the first time. Unless otherwise indicated, all software on FELICIA and CIAC has been scanned for known viruses, but it is advisable to scan all downloaded software using 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 scanning software cannot currently detect a virus within an application until it is in an executable form.

DOWNLOADING CONSIDERATIONS

If you are downloading to a Macintosh, be sure to use the Text version of the downloading protocol (e.g., Text-XMODEM, Text-YMODEM, etc., for downloads from FELICIA and ASCII mode on CIAC) on your Macintosh when downloading pure text files or unformatted documents. The text version of the downloading protocol corrects for the difference in the end of line characters used on the PC and Macintosh systems (the PC wants a CR-LF at the end of a line while the Macintosh wants a CR only.) When downloading a binary Macintosh file such as a program file or a formatted document, be sure to set the MacBinary form of the protocol (e.g., MacBinary-XMODEM for downloads from FELICIA, and Binary mode on CIAC) on your Macintosh. If you forget to do this, you can still do the conversion later using the Apple File Exchange utility included with the Macintosh system.

CIAC Electronic Bulletin Board and ftp Summary Guide, Continued

Downloadable 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. Be sure to use a binary downloading capability (e.g., XMODEM) for the executable files and archives. Files in ZIP archives must be extracted after downloading with PKUNZIP before they can be used. Macintosh files in SIT archives must be extracted with Stuffit before they can be used. Macintosh files in .CPT archives must be extracted with Compactor or Extractor. SEA files are self extracting archives and need no archiving program. Archiving utilities for both PC and Macintosh files are available in their respective file sections.

USING SHAREWARE

If you are using a shareware package downloaded from FELICIA or 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.

DOCKMASTER Resource Guide

This guide was provided by the NCSC.

DOCKMASTER has a multitude of resources concerning computer security available to our users. These resources include papers on viruses and other related issues, Internet resources, technical guidelines (Rainbow Series books and pamphlets), and forum meetings. The following information is available to most users on the DOCKMASTER system. To review the documents listed, the user can change his/her working directory to the indicated directory. The command to do this is “cwd pathname” where the pathname will be given above each list of documents in that directory. The “list” command will display the contents of that directory.

example: cwd >site>net>papers

>site>net>papers

- . Virus frequently asked questions
- . Site security handbook
- . GAO report on the Internet Worm incident
- . Virus101
- . NIST paper on computer viruses and related threats
- . Improving Unix systems security
- . GOSIP draft 2

>site>net>Internet

- . All kinds of information on Internet resources including what it is, its uses, a new user's guide and many more.

>site>net>irg

- . Several directories containing the chapters from the Internet Resources Guide

>site>net>rfcs

- . Many Request for Comments (RFC) documents. These documents cover subjects ranging from protocols for system to system communications; standards for network managers; X.400 and other protocols; addressing schemes; etc. The main library is located at the Network Information Center better known as the NIC. There is an index of all RFCs located at the NIC in this directory.

>site>pubs

- . Orange book in Hypercard version 2.01

DOCKMASTER Resource Guide, Continued

>site>pubs>criteria

- . ITSEC (Information Technology Security) paper
- . MSRF (Minimum Security Fundamental Requirements) paper
- . FC-Scope paper - a joint statement by the NIST and NSA on the Federal Criteria.

>site>pubs>guidelines

- . Trusted Database Interpretation (TDI)
- . Trusted Distribution Guidelines (TD)
- . Audit in Trusted Systems
- . Computer Security Subsystems
- . Computer Viruses
- . Configuration Management
- . Degausser Product List
- . Design Documentation
- . Discretionary Access Control
- . Endorsed Tools List
- . Formal Verification Systems
- . Glossary of COMPUSEC Terms
- . Guideline for Vendors
- . Office Automation Guideline
- . Password Management
- . Product Evaluation Questionnaire
- . Rating Maintenance Plan (RAMP)
- . TCSEC-85 (orange book)
- . TCSEC-83 (orange book)
- . Trusted Facility Management
- . Trusted Network Interpretation (TNI)

DOCKMASTER Resource Guide, Continued

The following forums are publicly available. To access any of these forums, enter the forum subsystem by typing “forum”. At the forum prompt, type the command “go” followed by either the long forum name or the short forum name. The first entry in the forum usually describes the nature of the forum and what information one may expect to find there. To get more information on how to read the forum entries, refer to the New User’s Guide to Multics sent with your account, send mail to “sysadmin”, or call the DOCKMASTER office. There are several other non-compusec related forum meetings that the DOCKMASTER user may be interested in. To get a list of these meetings, type “list_meetings” or “lsm” at the forum prompt.

<u>Long FORUM Name</u>	<u>Short FORUM Name</u>
CERT-TOOLS	cert-tools
Compusec_Papers_Database	cp
Computer_Security_Day	day
Conferences	conf
Criteria	criteria
DDN-News	ddn-news
ETHICS-L	ethics
IEEE_Cipher	cipher
Legislative_Issues	li
NBS_Conference	nbs
Nuance_Discussion	nuance
RISKS	risks
Security_Discussion	sd
Site_Security_Policy	site-sec
Tech_Guidelines_Info_Forum	tgif
Training_courses	tc
VIRUS-L	virus
WG-Security	wgs
announce	(no short name)
cert/accreditation	certify
epl	(no short name)
privacy_enhanced_mail	pem
privacy-digest	pd
privacy-issues	privacy

There is a menu driven program on DOCKMASTER that has information from the Products and Services catalog. To access that information just type “openair” and follow the directions on the screen. To create the menu, however, the user must have the PC or workstation terminal emulation software set to one that Multics supports for menu creation. The most popular ones are heath-19, vt100, vt102, and pcxt. A complete list can be viewed by typing “print >doc>iml_info>video_supported_list”. The openair program will ask for this information if it is required to draw the menu.

Mail Example

This example begins from the Unix command prompt `>`. User entries are shown in ***bold italics***. The entries are from two accounts: *richard* and *feingold*, indicated by the square bracketed remarks.

[As richard]

`> mail feingold`

Subject: ***workshop demonstration***

Well, do you think this will work? Remember to type control-d at the end. Okay?

`<control-d>`

EOT

[As feingold]

`> mail`

Mail version SMI 4.0 Wed Feb 7 23:10:16 PST 1990 Type ? for help.

“/usr/spool/mail/feingold”: 3 messages 2 new 3 unread

U 1 krww@cert.org Mon Nov 16 14:35 936/38857 VIRUS-L Digest V5 #180

>N 2 richard Mon Nov 16 15:11 12/301 Re: test

N 3 richard Mon Nov 16 15:19 14/358 workshop demonstration

`& 3`

Message 3:

From richard Mon Nov 16 15:19:21 1992

Return-Path: <richard>

Received: by (4.1/SMI-4.1)

id AA00471; Mon, 16 Nov 92 15:19:20 PST

Date: Mon, 16 Nov 92 15:19:20 PST

From: richard (RAF)

Message-Id: <9211162319.AA00471@>

To: feingold

Subject: workshop demonstration

Status: R

Well, do you think this will work? Remember to type control-d at the end. Okay?

`& r`

To: richard

Subject: Re: workshop demonstration

Why did you send me this?

`<control-d>`

EOT

`& h`

U 1 krww@cert.org Mon Nov 16 14:35 936/38857 VIRUS-L Digest V5 #180

N 2 richard Mon Nov 16 15:11 12/301 Re: test

> 3 richard Mon Nov 16 15:19 14/358 workshop demonstration

`& s workshop_msg`

“workshop_msg” [New file] 14/368

`& q`

`>`

eff Anonymous ftp Example

This example begins from the Unix command prompt >. User entries are shown in ***bold italics***.

```
> ftp ftp.eff.org
Connected to kragar.eff.org.
220 kragar.eff.org FTP server (Version 6.9 Tue Jul 7 15:53:04 EDT 1992) ready.
Name (ftp.eff.org:feingold): anonymous
331 Guest login ok, send E-mail address as password.
Password: feingold@local.sub.gov
230-If your ftp client chokes on this message, log in with a '-' as the
230-first character of your password to disable it.
230-
230-If you have problems with or questions about this service, send mail to
230-ftphelp@eff.org; we'll try to fix the problem or answer the question.
230-
230-Electronic Frontier Foundation newsletters and other information are in
230-pub/EFF and subdirectories thereof. If you're interested in official
230-EFF positions and philosophies, look here.
230-
230-For general information on the EFF, get pub/EFF/about-eff.
230-
230-Please read the file README
230- it was last modified on Sat May 2 18:10:09 1992 - 193 days ago
230 Guest login ok, access restrictions apply.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
etc
pub
bin
users
ls-lR.Z
.notar
README
226 Transfer complete.
47 bytes received in 0.011 seconds (4.3 Kbytes/s)
ftp> get README
200 PORT command successful.
150 Opening ASCII mode data connection for README (279 bytes).
226 Transfer complete.
local: README remote: README
285 bytes received in 0.0027 seconds (1e+02 Kbytes/s)
ftp> cd pub
250 CWD command successful.
ftp> cd CUD
250 CWD command successful.
ftp> ls
200 PORT command successful.
```

eff Anonymous ftp Example, Continued

150 Opening ASCII mode data connection for file list.

Added

Index

.notar

cdugd

alcor

ane

ati

bootlegger

ccc

chalisti

cdc

cpi

cud

dfp

fbi

inform

law

lod

misc

narc

networks

nfx

nia

nsa

papers

phantasy

phrack

phun

pirate

ppp

schools

synd

tap

upi

wview

aotd

Index.~1~

Added.~1~

Added.~2~

Index.~2~

226 Transfer complete.

280 bytes received in 0.037 seconds (7.4 Kbytes/s)

ftp> **cd bootlegger**

250 CWD command successful.

ftp> **ls**

200 PORT command successful.

150 Opening ASCII mode data connection for file list.

bootlegger-6

bootlegger-7

226 Transfer complete.

28 bytes received in 0.0032 seconds (8.6 Kbytes/s)

eff Anonymous ftp Example, Continued

```
ftp> get bootlegger-7  
200 PORT command successful.  
150 Opening ASCII mode data connection for bootlegger-7 (101274 bytes).  
226 Transfer complete.  
local: bootlegger-7 remote: bootlegger-7  
103885 bytes received in 56 seconds (1.8 Kbytes/s)  
ftp> quit  
221 Goodbye.
```

rn Example

This example begins from the Unix command prompt stc06>. User entries are shown in ***bold italics***.

stc06> ***rn***

Unread news in ornl.education.general	111 articles
Unread news in ornl.mail.decstation-managers	21 articles
Unread news in ornl.mail.framers	141 articles
Unread news in ornl.mail.info-afs	57 articles
Unread news in ornl.mail.report-card	15 articles

***** 111 unread articles in ornl.education.general--read now? [ynq]***n***

***** 15 unread articles in ornl...read now? [ynq] ***g alt.bbs.lists***

***** 152 unread articles in alt.bbs.lists--read now? [ynq]***y***

Article 402 (151 more) in alt.bbs.lists:

From: delivery@ixgch.imp.com (Ixgate Delivery)

Newsgroups: ch.general,chcon.general,de.etc.lists,alt.bbs.lists,alt.bbs,comp.bbs
.misc,xgp.general

Subject: BBS-List of Switzerland (October 1992)

Date: 14 Oct 92 01:06:20 GMT

Followup-To: ch.general

Distribution: world

Lines: 976

The BBS-List Service of XGP Switzerland

distributing the Swiss BBS-List on the Internet!
(See end of document for more details on this service.)

BOT

BYTE RIDER's DREAM BBS LIST OF SWITZERLAND ***** OCTOBER 1992
USRobotix oder nix!

Computers by AMIGA, Modems by USRobotics, support by MTV

--MORE--(2%)***g***

***** 2 unread articles in alt.bbs.lists.d--read now? [ynq] ***g comp.risks***

***** 8 unread articles in comp.risks--read now? [ynq]***y***

Article 142 (7 more) in comp.risks (moderated):

From: risks@CSL.SRI.COM (RISKS Forum)

Subject: RISKS DIGEST 13.86

Date: 24 Oct 92 20:39:50 GMT

Distribution: world

Organization: The Internet

Lines: 602

RISKS-LIST: RISKS-FORUM Digest Saturday 24 October 1992 Volume 13 : Issue 86

rn Example, Continued

FORUM ON RISKS TO THE PUBLIC IN COMPUTERS AND RELATED SYSTEMS
ACM Committee on Computers and Public Policy, Peter G. Neumann, moderator

Contents:

Software Bombs Out -- Ark Royal revisited (Simon Marshall)
Erased Disk used against Brazilian President (Geraldo Xexeo)
The NSF Net cable-cut story (Steve Martin via Alan Wexelblat)
Risks in Banking, Translation, etc. (Paul M. Wexelblat)
Re: 15th National Computer Security Conference (Dorothy Denning)
Re: Vote Early, Vote Often (Louis B. Moore)
T*p S*cr*t (Berry Kercheval)
Book Review: The Hacker Crackdown (David Barker-Plummer)
Filling station POS terminals: credit card users beware! (Steve Summit)
Int Workshop on Fault and Error Models of Failures in Comp Sys (Ram Chillarege)
--MORE--(4%)
End of article 142 (of 149)--what next? [npq] s

File /usr/u1/fgq/News/Comp.risks doesn't exist--
use mailbox format? [ynq]y
Saved to mailbox /usr/u1/fgq/News/Comp.risks
End of article 142 (of 149)--what next? [npq]q

***** 194 unread articles in comp.robotics--read now? [ynq]q
stc06>

NIST Dial Up Electronic Bulletin Board System Example

In this example, access is via a Hayes compatible modem. User entries are shown in *bold italics*. Note that the NIST electronic bulletin board system can also be accessed via ftp.

atdt 3019485717

RRING

CONNECT 2400

Welcome to NIST CSRC BBS - Node 2 (Reliable)

For faster login, enter FIRSTNAME LASTNAME PASSWORD

What is your FIRST name?

What is your LAST name? **Richard Feingold**

Checking Users...

User not found

Are you 'RICHARD FEINGOLD' ([Y],N)? **y**

What is your CITY and STATE? **Livermore, CA**

Welcome to the National Institute of Standards and Technology -

[...disclaimer/responsibility information deleted...]

by the National Institute of Standards and Technology.

* * * * *

RICHARD FEINGOLD from LIVERMORE, CA

C)hange FIRST name/LAST name/CITY and STATE, D)isconnect, [R]egister? **r**

Enter PASSWORD you'll use to logon again (dots echo)? **mypassword**

Re-Enter password for Verification (dots echo)? **mypassword**

Please REMEMBER your password

Welcome to RBBS-PC, Richard. Your security level 5 indicates that you have sufficient security to access this BBS. You have 60 (mins:secs) for this session.

Logging RICHARD FEINGOLD

RBBS-PC 17.3C Node 2, operating at 2400 BAUD-R,N,8,1

Telling sysop you're on...

Welcome to the NIST Computer Security Bulletin Board

This Bulletin Board is maintained by the Computer Systems Laboratory and is intended to encourage the sharing of information that will help users and managers better protect their data and systems. The mention of vendors or product names does not imply criticism or endorsement by the National Institute of Standards and Technology or by the SYSOP.

Sysop: Marianne Swanson

Technical Questions: John Wack

Voice: (301) 975-3359

NIST Dial Up Electronic Bulletin Board System Example,

Continued

```
301-948-5717 --> 300/1200/2400 Node 1
               --> 300/1200/2400 Node 2
301-948-5140 --> 1200/2400/9600 Node 3
               --> 1200/2400/9600 Node 4
```

Internet: telnet to cs-bbs.ncsl.nist.gov (129.6.54.30)
download files available via anonymous ftp
from csrc.ncsl.nist.gov (129.6.54.11)

* Note: by continuing, you explicitly acknowledge that all messages,*
* private and public, may be read by others, including the sysop(s).*

* Ctrl-K(^K) / ^X aborts. ^S suspends ^Q resumes *

***** NEWS *****
February 18, 1993

The draft Federal Criteria is now available in ascii. Bulletin 39
describes the document and lists all of the available formats for
More [Y]es,N)o,C)ont,A)bort,J)ump? y

downloading.

NIST Special Publication 800-5 and 800-6 are also now available in
ascii. Several new alerts have been posted as well as a proposed
guideline on sentencing criminals.

We have been having periodic problems with our Internet connection.
Efforts are being made to correct the situation.

At least 0 NEW file(s) since last on

* Ctrl-K(^K) / ^X aborts. ^S suspends ^Q resumes *

BULLETIN TOPICS MENU

- | | | |
|---|---------------------------------|--|
| 1 | Using the BBS - READ THIS! | NOTE: Viewing Bulletins is NOT straightforward! The BBS makes you view all bulletins from this menu only. For example, after displaying sub-menu 1 you want to view Bulletin 16, return to this menu and then enter '16' at the prompt at the bottom of this menu. |
| 2 | Computer Security Alerts | |
| 3 | NIST Publications | |
| 4 | Upcoming Events & Activities | |
| 5 | Of General Interest | |
| 6 | Resources | TO DOWNLOAD BULLETINS, first note the bulletin numbers. Quit this menu, go to the Main Menu & type 'F' to go to the File Menu. Then type 'D' to download. To download Bulletin 24, ex., use filename 'BULLET24' |
| 7 | Computer Security Organizations | |
| 8 | Virus-L and Risks Forum | |

Read what bulletin(s), L)ist, S)ince, N)ews ([ENTER] = none)? 2

NIST Dial Up Electronic Bulletin Board System Example,

Continued

* Ctrl-K(^K) / ^X aborts. ^S suspends ^Q resumes *

Computer Security Alerts (2)

The Alerts are placed in chronological order according to the date -- most recent at the top of the list. There are nine bulletins listed at any given time. The old bulletins are located in the file section under the "Alerts" Directory. The old bulletins can only be viewed by downloading them.

Date -----	Topic -----	Bulletin # -----
02-18-93	Revised Commodore Amiga UNIX finger Vulnerability CERT Advisory	29
02-17-93	Failure to disable user accounts for VMS 5.3 to 5.5-2 CIAC Information Bulletin	21

More [Y]es,N)o,C)ont,A)bort,J)ump? **n**

[...Menu repaint omitted...]

Read what bulletin(s), L)ist, S)ince, N)ews ([ENTER] = none)? **1**

* Ctrl-K(^K) / ^X aborts. ^S suspends ^Q resumes *
Using the BBS (1)

The following bulletins contain information on how to use this bbs. It is advisable to read these bulletins first before attempting to use the board. The instructions for downloading bulletins and files offers a step by step approach that should prove very useful.

Bullet # -----	Last Updated -----	Topic -----
11	09-28-89	General Information
12	03-25-92	Accessing the BBS
13	11-21-91	About Bulletins
14	11-21-91	About Files
15	09-28-89	Messages to the "Sysop"
16	03-25-92	Download and FTP Bulletins and Files
17	03-27-90	Upload Policy
18	02-06-92	Obtaining this BBS software

****NOTE:** An extensive User's Guide is available by either contacting Clare Lucey at 301-975-3359 or by downloading the file "BBSGUIDE.TXT" from this BBS.

* Ctrl-K(^K) / ^X aborts. ^S suspends ^Q resumes *

NIST Dial Up Electronic Bulletin Board System Example,

Continued

[...Menu repaint omitted...]

Read what bulletin(s), L)ist, S)ince, N)ews ([ENTER] = none)?<cr>
Checking messages in MAIN... ..
Sorry, RICHARD, No mail for you

RBBS-PC 17.3C Node 2

Caller # 63477 # active msgs: 719 Next msg # 2899

```

-----*>>> RBBS-PC MAIN MENU <<<*-----
----- MAIL ----- SYSTEM ----- UTILITIES ----- ELSEWHERE ---
[E]nter Messages [A]nswer Questions [H]elp (or ?)
[K]ill Messages [B]ulletins [F]iles
[P]ersonal Mail [C]omment to Sysop [G]oodbye
[R]ead Messages [I]nitial Welcome [X]pert on/off [Q]uit
[S]can Messages [U]tilities
[T]opic of Msgs [W]ho's on * = unavailable
-----
Current time: 11:19 AM Minutes remaining: 55 Security: 5
-----
MAIN: 55 min left
MAIN command <?,A,B,C,E,F,G,H,I,K,P,Q,R,S,T,U,V,W,X>? g
Log off (Y,[N])? y
```

Now: 03-02-1993 at 11:20:54
On for 5 mins, 54 secs
60 min left for next call today
RICHARD, Thanks and please call again!

CIAC Anonymous ftp Example

This example begins from the Unix command prompt >. User entries are shown in ***bold italics***. Note that the name *CIAC* will be changing to *ciac*.

> ***ftp CIAC***

Connected to CIAC.llnl.gov.

220 CIAC.llnl.gov FTP server (Version 6.22 Wed Jan 27 09:36:28 PST 1993) ready.

Name (CIAC:feingold): anonymous

331 Send e-mail address, name, organization, and phone number as password.

Password: ***feingold@sub.domain.gov, Richard Feingold, CIAC, 510.555.1212***

230- This is the CIAC archive, provided and maintained by

230- the Computer Security Group, Lawrence Livermore National

230- Laboratory.

230-

230- All activity is logged with your host name and e-mail 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.

ftp> ***ls***

200 PORT command successful.

150 Opening ASCII mode data connection for file list.

lost+found

etc

bin

pub

usr

dev

.login_message

0-index.txt

incoming

226 Transfer complete.

76 bytes received in 0.016 seconds (4.8 Kbytes/s)

ftp> ***cd pub***

250 CWD command successful.

ftp> ***ls***

200 PORT command successful.

150 Opening ASCII mode data connection for file list.

spi

ciac

felix

tmp

util

sun

patches

CIAC Anonymous ftp Example, Continued

```
226 Transfer complete.
43 bytes received in 0.011 seconds (3.9 Kbytes/s)
ftp> cd ciac
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
virus-l
news.txt
docs
.private
pcvirus
pcutils
macvirus
macutils
atarivir
reviews
books
ciacdoc
certdoc
ddndoc
nasaspan
nistdoc
ihg
226 Transfer complete.
149 bytes received in 0.023 seconds (6.2 Kbytes/s)
ftp> pwd
257 "/pub/ciac" is current directory.
ftp> cd ciacdoc
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
fy89
a-fy90
b-fy91
c-fy92
d-fy93
xref.txt
226 Transfer complete.
48 bytes received in 0.0097 seconds (4.8 Kbytes/s)
ftp> cd d-fy93
250 CWD command successful.
ftp> ls
200 PORT command successful.
150 Opening ASCII mode data connection for file list.
d-01.ciac-novel-access-rights
d-02.ciac-(*limited-distribution*)
d-03.ciac-vms-MONITOR-patch
d-04.ciac-sunos-18-patches
0-index.txt
```

CIAC Anonymous ftp Example, Continued

```
intro.txt-introduction-to-CIAC
ciacreqs.txt-ciace_doe_requirements
d-05.ciac-hp-NIS-ypbind
226 Transfer complete.
230 bytes received in 0.016 seconds (14 Kbytes/s)
ftp> get d-03.ciac-vms-MONITOR-patch
200 PORT command successful.
150 Opening ASCII mode data connection for d-03.ciac-vms-MONITOR-patch (7249 bytes).
226 Transfer complete.
local: d-03.ciac-vms-MONITOR-patch remote: d-03.ciac-vms-MONITOR-patch
7382 bytes received in 0.12 seconds (61 Kbytes/s)
ftp> bye
221 Goodbye.
>
```

CIAC Electronic Bulletin Board System Example

In this example, access is via a Hayes compatible modem. User entries are shown in ***bold italics***. Note that the electronic bulletin board system can also be accessed via ftp.

atdt 5104234753

RRING

CONNECT 2400

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

WELCOME TO FELICIA

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

First Name? ***Richard***
Last Name? ***Feingold***
Searching User File ...
Calling from (City,State)? ***Livermore, CA***

TBBS Welcomes RICH FEINGOLD
Calling From LIVERMORE, CA
Is this correct? ***y***
Chars per line on screen(10-132)? ***80***

<A>VIDTEX	TRS-80 1/3	<C>VT-52	<D>ATARI	<E>H19/H89/Z19
<F>IBM PC	<G>Televid 925	<H>VT-100	<I>Mac Versater	<J>Dum TTY

Enter letter of your terminal, <CR> if not listed: ***h***

Terminal Profile Set to:
No ANSI codes Allowed
No IBM Graphics Allowed

Upper/Lower Case
Line Feeds Needed
0 Nulls after each <CR>
Do you wish to modify this? ***N***
Do you wish to have a pause after each display page (Y/N)? ***N***

Please Enter a 1-8 character Password to be used for future logons. This password may have any printable characters you wish. Lower case is considered different from upper case and imbedded blanks are legal. REMEMBER THIS PASSWORD. You will need it to log on again.

Your password? ***mypswd***
You have read through message 0
Current last message is 191
You are caller number 1726
You are authorized 60 mins this call

CIAC Electronic Bulletin Board System Example, Continued

Policies of Felix

[...Policy and disclaimer omitted...]

```
| The Computer Incident Advisory Capability Bulletin Board
| Voice:Com/FTS (510)422-8193
| Data:Com/FTS (510)423-4753 2400 baud
| Com/FTS (510)423-3331 9600 baud
| Your friendly Sysops are Bill and Karyn
+-----
```

This board is run by CIAC for the Department of Energy.

```
[...Informational messages omitted...]
```

New User Registration Section

Do you work for a DOE site?

<Y>es

 $\langle N \rangle > 0$

<S>kip registration.

Command: **y**

Registration for DOE sites.

Enter your full name: **Richard Feingold**

Organization: **LLNL**

Address Line 1: **L-303**

Address line 2: **P.O. Box 808**

City, State, ZIP:**Livermore, CA 94551**

Commercial Telephone Number: **510.422.1783**

FTS Telephone Number: **510.422.1783**

Responsible DOE field office (SAN, ID, etc.):**SAN**

Richard Feingold

LLNL

L-303

P.O. Box 808

Livermore, CA 94551

510.422.1783

510,422,1783

SAN

Is this correct (Y/N)?y

FELICIA BBS - Main Menu

Computer Incident Advisory Capability

<*> Information on TBBS

<N>ew Files On Felicia

Bulletins and System Notices

<F>ile Transfer Section

<M>ail and dialog with Felix users

<V>irus Database

<R>ecent callers

<T>ime on the system

Utilities Section

<G>oodbye

CIAC Electronic Bulletin Board System Example, Continued

Command: **f**

FELICIA BBS - File Transfer Section
Computer Incident Advisory Capability
=====

<D>ownload Area
<U>pload Area
<->Previous Menu
<T>ime on the system
<G>oodbye

Command: **d**

FELICIA BBS - File Download Section
Computer Incident Advisory Capability
=====

Select A Download Area From The Following List

<M>acintosh Files
Macintosh<h> Utility Programs
<P>C Files
PC <U>tility Programs
<A>tari files
<L> Incident Handling Guidelines
<C>IAC Documents
<E>RT Documents
<N>IST Documents
<D>DN Documents
NA<S>A-SPAN documents
<V>irus-L Moderated News
<R>evIEWS of anti-virus software
<O>ther useful stuff.
<->Previous menu
<T>ime on the system
<G>oodbye

Command: **o**

Type P to Pause, S to Stop listing

ETC DIRECTORY

This directory contains useful things that don't fit into our other categories.

----- Notices and Guides -----

BIBLIO.TXT	3463	2-05-92	Bibliography of virus books.
GRADSCH.TXT	3537	12-09-91	Grad schools with Comp Security Progs.
CIACDB.ZIP	110025	3-25-91	CIAC virus database (big)
DES.TXT	22455	1-30-90	General information on DES encryption
FATHER_X.TXT	41966	1-11-90	A full report on the Father Xmas worm
GUIDANCE.TXT	13568	12-17-84	General guidance on computer security
FTPSITES.TXT	35737	1-11-90	Common FTP sites on the Internet

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

CIAC Electronic Bulletin Board System Example, Continued

FELICIA BBS - File Download Section
Computer Incident Advisory Capability
=====

Select A Download Area From The Following List

<M>acintosh Files
Macintos<h> Utility Programs
<P>C Files
PC <U>tility Programs
<A>tari files
<L> Incident Handling Guidelines
<C>IAC Documents
C<E>RT Documents
<N>IST Documents
<D>DN Documents
NA<S>A-SPAN documents
<V>irus-L Moderated News
<R>evIEWS of anti-virus software
<O>ther useful stuff.
<->Previous menu
<T>ime on the system
<G>oodbye

Command: **g**

FELICIA BBS - Termination Section
Computer Incident Advisory Capability
=====

Do you want to leave a message for the
SYSOP?

<Y>es
<N>o

<->Return to previous menu

Command: **n**

Logged on at 13:17:45
Logged off at 13:20:38

Thanks for calling FELICIA
Please Hang Up Now

References

Cronin, Mary J., *Doing Business on the Internet*, Van Nostrand Reinhold, 1994.

Fraase, Michael, *The MAC Internet Tour Guide*, Ventana Press, 1993.

Frey, Donnalyn & Adams, Rick, *!%@:: A Directory of Electronic Mail Addressing and Networks*, O'Reilly & Associates, Inc., 1990.

Krol, Ed, *The Whole Internet User's Guide and Catalog*, O'Reilly & Associates, Inc., 1992.

LaQuey, Tracy, with Ryer, Jeanne C., *The Internet Companion—A Beginner's Guide to Global Networking*, Addison Wesley, 1993

Marine, April, editor, *Internet: Getting Started*, SRI International, 1992.

Network Information Center, *DDN NEW USER GUIDE*, anonymous FTP from nic.ddn.mil:netinfo/nug.doc.

Quarterman, John S., *The Matrix: Computer Networks and Conferencing Systems Worldwide*, Digital Press, 1990.

Appendix B: Contacting CIAC

Contacting CIAC

Phone	(510) 422-8193
Fax	(510) 423-8002
STU-III	(510) 423-2604
Electronic mail	ciac@llnl.gov
Emergency SKYPAGE	800-SKYPAGE pin# 855-0070
Anonymous FTP server	ciac.llnl.gov (IP 128.115.19.53)
BBS	(510) 423-3331 (9600 Baud) (510) 423-4753 (2400 Baud)

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 _____