U.S. DOE's Computer Incident Advisory Capability

CIAC NOTES

Number 94-03a July 6, 1994

CIAC is available 24-hours a day via its two skypage numbers. To use this service, dial 1-800-759-7243. The PIN numbers are: 8550070 (for the CIAC duty person) and 8550074 (for the CIAC manager). Please keep these numbers handy.

Welcome to the third issue of CIAC Notes! We are adding the year to the issue number to make referencing easier. Our guest author on Firewalls has promised future articles. And we've dropped the tables of PC and Mac Anti-Virus product updates from this issue in the interests of time and space. Let us know if you have topics you would like addressed or have feedback on what is useful and what is not. Please contact the editor, Allan L. Van Lehn, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

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

Table of Contents

Feature Articles	Internet Sniffer Update
	Social Engineering
	Firewalls
	Security Information and Resources via WWW
	Some Upcoming Computer Security Related Conferences
DEC user	ULTRIX and OSF/1 Patch Kits Available
PC user	CD-IT.ZIP Trojan
	Three New PC Viruses: Natas, Junkie, CHiLL TOUCH
MAC user	Defeating FileMaker Password Protection
CIAC information	CIAC Bulletins Issued Recently
	Subscribing to CIAC Electronic Publications
	Accessing CIAC's Electronic Information Servers
	Publications Available from CIAC
	Who is CIAC
	Contacting CIAC

Feature Articles

Internet Sniffer Update

Internet Sniffer attacks are still with us! Everyone, including the DOE and its contractors, is becoming more reliant on electronic communications. If you remotely log into a host system, you should consider changing your password weekly. You are especially at risk when login information travels over public networks such as the Internet. However, it is not just your login information that is at risk! Assume that whatever you send to your colleagues across the site, nation or world, can and may be seen by someone else. Today,

because E-mail is so convenient and rapid, users sometimes include sensitive information in the message body or in an attachment assuming it is safe. This should not be done! If you have not encrypted your message or your attachment, this information can be "grabbed" surreptitiously by a computer cracker. It also can be misdirected to someone other than the intended recipient. CIAC has seen instances of both. You may have heard of Privacy Enhanced Mail (PEM), Pretty Good Privacy (PGP) or other products from commercial vendors. Secure and authenticated E-mail is still being developed and waiting for standardization.

Conclusion: E-mail should not be used for sensitive discussions unless the messages and associated attachments are DES encrypted. Many DOE/DOE contractor sites already have established policies regarding the use of E-mail. Check with your site CPPM/CSSM to learn your organization's policy. To obtain further information, contact Sandy Sparks, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

Social Engineering

In today's world of computer crime, all perpetrators don't have to come in over the Internet; they may just as easily get information simply by asking. Beware of the friendly insider or the official sounding outsider; they may be playing on your good will or naiveté to get what they need. A few examples should help...

A technician answers the telephone. "Bill Jones, Telecom Operations."

"Hello. This is Martin White with AT&T Operations. We think someone may have broken into your PBX switch. Can I talk to the technical person in charge?"

"That's me," Bill says.

"How're you doing, Bill?"

"Good. And you?"

A deep breath. "Not too bad, except that it's Friday afternoon and I think we're going to have to wade through a mountain of paper. Anyway, as I was saying, we think your switch has been compromised."

"What makes you think so?"

"Your toll free dial in is 800-555-1212 isn't it?"

"Yeah."

"We alarmed on someone sequence dialing all the 555 numbers. The sequence stopped on yours, then randomly searched for dial out access codes. If they found it, you know how bad that can be."

"Well, can't you tell for certain?" Bill asks.

"Sure, I'm searching now, but it's so much paper." The sound of a page being flipped. "What scares me is that while I'm doing this, the bad guys could be selling your long distance on the streets right now. Maybe you better take your 800 service off line or change the access code."

"Jeez, I can't do that. The people in the field…our business depends on it."

Martin sighs. "That's too bad. The intruders may not have even cracked the code." The sound of another page being flipped and then fingers snapping. "Bill, I just thought of something. I have all this on line. It would just take a minute to search for your access code." A heavy sigh. "Why didn't I think of this before? It's been a long week—too many hours looking at numbers." A pause. "Okay, what's your access code?"

"I…er," Bill hesitates.

"Oh, yeah, you shouldn't give it out. I understand." The sound of another page being flipped. "It was such a good idea, too." Pause. "These guys sure tried a lot of permutations. These eight digit codes…" Another page.

"Hey," Bill says, "we could be here all night. Forget I told you this: the code is 98765432."

"Thanks. Great. Hold on." The sound of keys being typed. "Okay. Let me double check." More typing. "That's it. Good news, they never got to it." Pause. "Thanks a lot, Bill. We would have been here half the night for a non-event. By the way, once they pass you by, it's very rare that they'd come back. You're in good shape. Though you probably want to change that access code."

"Nah, that would be a real pain. Everyone in the field would have to be informed. Maybe I'll kick it up to the boss on Monday. Have a good weekend."

"You too."

"Martin White" will have a good weekend. He and his confederates will sell discount long distance service on the streets of New York City at public phone booths, a zero overhead pure profit enterprise. The costs to Bill's organization will be over $150,000. This is one (fictionalized but only too realistic) example of what's called "Social Engineering," an ironic characterization of the non technical aspect of Information Technology (IT) crime. In other human interactions it's called a "Con (or Confidence) Game" where Martin is the "Con Artist." The underlying idea is simple: deceive the victim into revealing secret information or taking inappropriate action for the attacker's benefit.

Most of us are helpful and trusting—it's human nature. We want to be good neighbors and have good neighbors. Americans are especially trusting and as foreign industrial espionage increases, we must check on requesters before we hand over either access or information. Social Engineers exploit this cooperative inclination. They also employ intimidation and impersonation as well as plain old fashioned snooping and eavesdropping.

A confused and befuddled person will telephone a clerk and ask for his password to be changed. An important sounding man identifying himself as an executive will telephone a new system administrator and demand access to his account NOW. A person at an airport will look over your shoulder ("shoulder surfing") as you key in your telephone credit card or ATM PIN (they even use binoculars and camcorders). A visitor will watch you type your username and password at your keyboard. A confident person will call up a computer operator and ask him or her to type in a few lines of instruction at the console. An attacker will sift through your paper trash ("dumpster diving"), looking for clues to unlock your IT treasures.

Unlike the technology it targets, social engineering is an old profession with a new name. It succeeds frequently because our culture has not caught up with its own technology. A social engineer would have a much more difficult time getting the combination to a safe than a password, or even the combination to a locker at the health club. The best defense is simple: it's education, training, and awareness. For further information, please contact Richard Feingold, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

Internet Firewalls

by Stephen P. Cooper, CSTC, LLNL

As more computers and larger networks get attached to the Internet, it gets more difficult to keep them secure from some of the hostile or curious elements on the Internet. An increasingly popular method of connecting to the Internet is through firewalls.

A firewall is a combination of hardware and software components that provide a choke point between a "trusted" network, such as an organizational network, and an "untrusted" network such as the Internet. The firewall provides a certain level of control as to what can go between the two networks.

Firewall technology has not yet reached the "turn-key" stage, although the number of commercial product announcements is increasing. There are several ways to make your own firewalls and there are a number of people and companies doing firewall consulting. There is also a lot of free software and advice available over the Internet. Several references are listed at the end of this article.

There are several different ways to configure a firewall. Two common hardware (and software) components are a screening router and an application gateway (also called a "bastion" host). The screening router provides the primary connection between a trusted and an untrusted network. It routes protocol packets and can be configured to block packets by hardware address, IP address, or TCP or UDP port in the case of those protocols. For example, the router can be configured to block incoming FTP requests and all NFS traffic. The screening router is limited to these low-level network functions, and many network applications have protocols too complex to be handled at this level. That is where an application gateway is used.

An application gateway is used to provide an extra layer of protection to certain network applications. For incoming Telnet or FTP connections, it may provide one-time password authentication to prevent an unauthorized user from capturing and reusing a password to get into the trusted network.

This is just a sample of the terminology and configuration possibilities of Internet firewalls. Because of the importance of this area in computer security, CIAC/CSTC will continue to investigate firewall configurations and technology and will produce a series of firewall articles in future issues of CIAC Notes. If you have questions or topics you would like to see covered, send mail to *ciac@llnl.gov*. Until then, the following are some good sources of information and discussion about firewall topics:

(1) Books

William R. Cheswick and Steven M. Bellovin. *Firewalls and Internet Security; Repelling the Wily Hacker.* Addison-Wesley, Reading, Massachusetts, 1994.

(2) Anonymous FTP Information

Ftp.greatcircle.com - Firewalls mailing list archives.
Directory: pub/firewalls

Ftp.tis.com - Internet firewall toolkit and papers.
Directory: pub/firewalls

Research.att.com - Papers on firewalls and breakins.
Directory: dist/internet_security

Net.Tamu.edu - Texas AMU security tools.
Directory: pub/security/TAMU

(3) Mailing Lists

The Internet firewalls mailing list is a forum for firewall administrators and implementors. To subscribe to Firewalls, send "subscribe firewalls" in the body of a message (not on the "Subject:" line) to "Majordomo@GreatCircle.COM". Archives of past Firewalls postings are available via anonymous FTP from ftp.greatcircle.com in pub/firewalls/archive.

Security Information and Resources via WWW

The following information from a recent posting to the firewalls mailing list (see the above article) was provided by Rodney Campbell, Telecom, Australia, who has created a World Wide Web page. It is an index to sources of network and computer security information. The index currently contains pointers to the following topics:

Frequently Asked Questions
WWW Information Sources
USENet News Groups
FTP Sites
Mailing Lists & Mail Addresses

The Uniform Resource Locator (URL) for the index is

http://www.tansu.com.au/Info/security.html

Or if you are reading this with a web browser:

<A HREF="http://www.tansu.com.au/Info/security.html">
Security Reference Index</A>

Note: The index has some Australian touches to it.

Upcoming computer security related conferences

Sixth Annual Computer Security Incident Handling Workshop
Boston Park Plaza Hotel
Boston, Massachusetts
July 25 - 29, 1994
Sponsored by: Forum of Incident Response and Security Teams (FIRST)

Since November of 1988, there has been an almost continuous stream of security-related incidents that have affected thousands of computer systems and networks throughout the world. To address this threat, a growing number of government and private sector organizations in North America, Europe and Australia have worked together to exchange information and coordinate response activities. This coalition, known as FIRST, brings together a variety of computer security incident response teams from the government, commercial, and academic organizations. FIRST aims to foster cooperation and coordination in incident prevention, to prompt rapid reaction to incidents, and to promote information sharing among members and the community at large.

Focus
The focus of this year's workshop is on tools for incident handling in an international arena. The workshop is being conducted as a series of tutorials, seminars, and hands-on sessions on related topics. Two all day tutorials stressing basic network security and incident handling issues will be available for all participants on the first day. A half day of working groups sharing information, requirements and guidance in an informal interactive environment will be held on the second day. Groups will produce notes and/or documents to be shared with other workshop attendees. The workshop will begin in the afternoon of the second day with presentations focusing on tools that are utilized in incident handling. As part of the registration fee, all participants will receive a CD-ROM containing many of the tools discussed at the workshop that includes but is not limited to:
• Advisories
• Mailing list archives
• Security related papers and documents
• Password security software
• Network security software
• Firewalls software
• Authentication software

Preliminary Agenda
• Tutorials: Security for Managers, Incident Handling for Techies
• Working Groups: Collecting Computer Crime Statistics, Internet Security/Insecurity, FIRST Membership Responsibilities
• Introduction of incident handling teams
• Discussion of non-traditional and public domain network servers
• Vendor panel on how vendors respond to incident response teams
• Panel discussion on interoperability in the FIRST community
• Invited talks on recent detection and analysis tools
• Panel on forming an incident response team
• Discussion of the trends in legal and administrative issues with a focus on international issues

Registration
The registration fee is $275.00 per person. Registration includes coffee breaks, two lunches, a reception, and workshop materials. In order to be pre-registered and have your name appear on a preliminary participants list, registration must be received by July 11, 1994. Requests for cancellations or refunds must be submitted in writing by July 11, 1994. For additional registration information, please contact Lori Phillips, NIST, 301-975-3881, Fax: 301-948-2067.

Additional Details
For additional technical information, contact Marianne Swanson or John Wack, NIST, 301-975-3359, E-mail: workshop-info@first.org.

DEC User Articles

DEC ULTRIX, DECnet ULTRIX and OSF/1 Patches Available

Digital Equipment Corporation has prepared Security Patch Kits for the following versions of ULTRIX Risc and VAX 4.3, 4.3A, 4.4; DECnet-ULTRIX 4.2; and OSF/1 1.2, 1.3,

1.3A, and 2.0 systems. These kits are available from DEC via normal software maintenance contract services, from your local office, or via anonymous FTP from ciac.llnl.gov. To obtain further information, contact Allan L. Van Lehn, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

PC User Articles

CD-IT.ZIP Trojan

In early May, a Trojan program was identified in the CD-IT.ZIP archive available via bulletin boards and Internet file transfer sites. Documentation in the archive indicated that these programs were from Chinon, a manufacturer of CD-ROM drives. However, they were not from Chinon, and Chinon issued a press release warning users to not use the software contained in the archive. The warning states that the archive contained a Trojan program that destroys the contents of hard disk drives. CIAC distributed that press release in its Information Bulletin E-20, issued May 6, 1994. We have since obtained a copy of the bogus CD-IT.ZIP archive and are analyzing its contents. The archive contains two programs, some documents, and data files.

WARNING: If you should find a copy of this archive, do not run the program INSTALL.COM, as it contains the Warpcom-2 Trojan.

The documentation contained in the archive claims that this is a utility program that will enable you to "READ and WRITE to your CD-ROM!" That statement in itself should be a tip-off that there is something wrong here, as it is physically impossible to write with a standard CD-ROM drive. Even writable CD's (CD-R) can only be written in a special drive that contains additional hardware. Scanning for the Trojan program with anti-virus scanners may not locate it, as most scanners look only for virus code, not Trojans. However, F-PROT version 2.10c does detect and identify this Trojan, and the upcoming release of DataPhysician Plus 4.0D will also detect it.

The Trojan program overwrites the copy of COMMAND.COM pointed to by the current COMSPEC environment variable. COMMAND.COM is overwritten with binary ones (Hex FF), except for a few bytes at the beginning. Those few bytes at the beginning of COMMAND.COM are a short program to overwrite the first 256 sectors of your D: drive with garbage. The next time the system needs to reload COMAND.COM, the small program trashes the D: drive and then the system crashes trying to execute invalid code. The hard disk then becomes unbootable, because COMMAND.COM is needed to boot the system. While we have not extensively examined the effects of the Trojan, the damage to the C: drive can be repaired by replacing the damaged copy of COMMAND.COM with a new, undamaged one. The damage to the D: drive may not be repairable, though you may be able to recover some of the files using a disk recovery program such as Norton Utilities, or PCTools.

Be sure to replace the correct copy of COMMAND.COM. The copy to replace is the one pointed to by the COMSPEC environment variable. To see the current value of COMSPEC, type SET followed by a Return. The default value is C:\COMMAND.COM, where C: is the boot drive (It will be the A: drive if you boot from a floppy). If you boot from a floppy drive to repair a system, the SET command will not show you the correct copy of COMMAND.COM to replace, as it will point to the copy of COMMAND.COM on the floppy disk. To find the correct copy of COMMAND.COM to replace, see if the value

of COMSPEC has been set in the CONFIG.SYS file on the hard disk. If it is not set there, then the copy of COMMAND.COM to replace is the one in the root directory of the C: drive. Note that there is usually a second copy of COMMAND.COM in the DOS directory on the C: drive, that can be copied into the root directory. Since the copy of COMMAND.COM is not necessarily run right away, you have a chance to save your D: drive. If after mistakenly running the INSTALL.COM program, your system seems to be running OK, immediately replace the copy of COMMAND.COM with a good one. If you can replace it before it is executed, your D: drive will not be overwritten.

Note: Chinon indicated that there is a legitimate program called CD-IT that is used with CD-ROM drives. If the documentation claims to give you *write* access to a CD-ROM, then you have the bogus archive. To obtain further information, contact William J. Orvis, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

Three new PC viruses: Natas, Junkie, CHiLL TOUCH

Natas

According to knowledgeable sources in the Anti-Virus (AV) community, this virus was written by the author of the Satan Bug virus (Natas is Satan backwards), and has many of the same characteristics. CIAC has received information that the Natas computer virus for MS-DOS/PC-DOS computers has been seen in the Los Angeles area. Previously this virus was known to be widespread in the Mexico City area.

Natas is a super-polymorphic, multipartite virus. A polymorphic virus changes how it looks with each new infection to make it difficult for an anti-virus signature scanner to detect it. A multipartite virus infects both programs and boot sectors. Natas also infects system (.SYS) programs and memory managers like QEMM and EMM386, causing those programs to report memory errors.

Most AV scanners should be able to detect this virus by name in the next release. Current AV program change detectors should be able to detect the presence of this virus now.

Junkie

Several press reports distributed over the Internet have raised speculation that a new, very dangerous computer virus named Junkie is spreading around the country. Unfortunately, those reports are exaggerating the importance of this virus by claiming that it is widespread and that it contains new technology that present anti-virus products cannot counter. Anti-virus authorities report that Junkie is a relatively unsophisticated virus with no new technology, and that the change detection (new virus) scanners in most anti-virus packages should detect it. The following is an excerpt from a Norton Anti-Virus (Symantec Corp.) press release that describes Junkie:

> "Junkie, which reportedly first infected a company in the Netherlands after being downloaded from a bulletin board, is a multipartite virus that infects hard drives or floppy disks and files. It writes the virus code to the Master Boot Record (MBR) on the hard drive, the DOS boot record on floppies, and only infects .COM files. Junkie is not a stealth virus. It is variably encrypted, but not polymorphic. No "trigger" or "payload" has been identified for the Junkie virus."

All AV change detectors will detect it, and all scanners should detect it by name in their next released version.

CHiLL TOUCH

The CHiLL TOUCH virus was found in some game programs on ZiffNet's Ziff Public Brand Software Arcade Forum which about forty people downloaded. If you obtained this software (listed below) between June 3rd and 14th, you should not run or redistribute it. Delete it and obtain new copies from ZiffNet. ZiffNet and Compuserve have tried to contact all the people that downloaded it. ZiffNet also said that the virus did not originate from any of these files and that versions of these programs downloaded before June 3rd are absolutely fine. The programs are:

Animated Clock (ACLOCK.ZIP)
John's Animated Computer Game (AJOHN.ZIP)
Animated Alphabet (ALPHA.ZIP)
Animated Memory Game (AMEM.ZIP)
BAT Commander (BATCMD.ZIP)
Big Red Self-Test (BRTEST.ZIP)
Dungeon, v9.0 (DUNGN.ZIP)
SHEZ, v10.0 (SHEZ.ZIP)
Stealth, v5.0 (STLTH.ZIP)

The CHiLL TOUCH virus is a resident .COM infector, affecting only .COM files larger than 64K. The payload is disabled because it appears that the virus writer was having trouble getting it to work. It is variably encrypted. It is not a stealth virus. It is not polymorphic. It does not infect the boot block of hard drives or floppy disks. To obtain further information, contact William J. Orvis, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

MAC User Articles

Defeating FileMaker Password Protections

CIAC has examined an application programmed to defeat the password protection scheme in Claris' FileMaker Databases (FileMaker II, FileMaker Pro v1.0 and v2.0) for the Macintosh. A DOS version may be available by the time you read this. This application is being distributed freely via several bulletin board systems. By using this application, anyone can modify (or modify a copy of) the database file. Any FileMaker database that can be seen on a network is at risk. This means that shared folders and/or files even if they are restricted to read-only access can be copied and altered to remove their password protection.

It is quite possible that other "password" protected databases are vulnerable to this kind of attack. You might want to question your software vendor about this before you select your next database engine. To obtain further information, contact Allan L. Van Lehn, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

CIAC Information

CIAC Bulletins Issued recently

CIAC issues two categories of computer security announcements: the information bulletin and the advisory notice. Information bulletins describe security vulnerabilities and recommend countermeasures. Advisory notices are more imperative, urging prompt action for actively exploited vulnerabilities. Advisory notices are delivered as quickly as possible via E-mail and FAX.

E-18 Bulletin	Sun Announces Patches for automountd Vulnerability	May 05, 1994, 1200 PDT
E-19 Advisory	nVir A Virus Found on CD-ROM	May 05, 1994, 1500 PDT
E-20 Bulletin	Trojan Attack on Chinon CD-ROM Drives	May 06, 1994, 1200 PDT
E-21 Bulletin	*Restricted Distribution*	May 11, 1994, 0845 PDT
E-22 Bulletin	*Restricted Distribution*	May 11, 1994, 0845 PDT
E-23b Bulletin	Vulnerability in HP-UX systems with HP Vue 3.0	May 17, 1994, 0930 PDT
E-24 Bulletin	Security Patch Kits for ULTRIX, DECnet-ULTRIX and OSF/1	May 18, 1994, 1530 PDT
E-25a Bulletin	BSD lpr Vulnerability in SGI IRIX	May 19, 1994, 1600 PDT
E-26 Advisory	UNIX /bin/login Vulnerability	May 23, 1994, 0700 PDT
E-27 Bulletin	*Restricted Distribution*	May 23, 1994, 1430 PDT
E-28 Bulletin	*Restricted Distribution*	May 26, 1994, 0930 PDT
E-29a Bulletin	IBM AIX bsh Queue Vulnerability Remote users may access a privileged account via the bsh batch queue. Disable the queue, then install a fix.	June 3, 1994, 1500 PDT
E-30 Bulletin	Majordomo distribution list administrator vulnerabilities Intruders may gain remote access to the Majordomo account and execute arbitrary commands. Upgrade to version 1.92.	June 15, 1994, 1400 PDT

To obtain further information, contact Allan L. Van Lehn, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

Subscribing to CIAC Electronic Publications

CIAC has several self-subscribing mailing lists for electronic publications:
1. CIAC-BULLETIN for Advisories, highest priority - time critical information and Bulletins, important computer security information;
2. CIAC-NOTES for Notes, a collection of computer security articles;
3. SPI-ANNOUNCE for official news about Security Profile Inspector (SPI) software updates, new features, distribution and availability;

4. SPI-NOTES, for discussion of problems and solutions regarding the use of SPI products.

Our mailing lists are managed by a public domain software package called ListProcessor, which ignores E-mail header subject lines. To subscribe (add yourself) to one of our mailing lists, send the following request as the E-mail message body, substituting CIAC-BULLETIN, CIAC-NOTES, SPI-ANNOUNCE or SPI-NOTES for *list-name* and valid information for *LastName FirstName* and *PhoneNumber*. Send

E-mail to `ciac-listproc@llnl.gov:`
`subscribe` *`list-name  LastName, FirstName PhoneNumber`*
e.g., `subscribe ciac-notes O'Hara, Scarlett W. 404-555-1212 x36`

You will receive an acknowledgment containing address, initial PIN, and information on how to change either of them, cancel your subscription, or get help. To subscribe an address which is a distribution list, first subscribe the person responsible for your distribution list. You will receive an acknowledgment (as described above). Change the address to the distribution list by sending a second E-mail request. As the body of this message, send the following request, substituting valid information for *list-name*, *PIN,* and *address of the distribution list*:. Send

E-mail to `ciac-listproc@llnl.gov:`
`set` *`list-name`* `address` *`PIN  distribution_list_address`*
e.g., `set ciac-notes address 001860 remailer@tara.georgia.orb`

To be removed from this mailing list, send the following request:
unsubscribe *list-name*

For more information, send the following request:
help

If you have any questions about this list, you may contact the list's owner: listmanager@cheetah.llnl.gov.

Accessing CIAC's Electronic Information Servers

CIAC operates two file server systems for the DOE community: the CIAC Bulletin Board System (CIAC BBS) and an anonymous File Transfer Protocol (FTP) server, also named CIAC. CIAC BBS used to be named FELICIA and before that, FELIX. The BBS is accessible via telephone using a modem. The FTP server is accessible via the Internet. Both of these file servers contain all of the publicly available CIAC, CERT/cc, NIST, and DDN bulletins, virus descriptions, the virus-l moderated virus bulletin board, copies of public domain and shareware virus detection/protection software, copies of useful public domain and shareware utility programs, and patch files for some operating systems.

The CIAC BBS

Our BBS is accessed via analog telephone line, a modem, and a terminal or computer running a terminal emulator program. Set your modem transmission protocol to 8 bit, no parity, one stop bit. The access numbers are:

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

The first time you call in, please 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.

The FTP server ciac.llnl.gov

The new name of our Internet FTP server is ciac.llnl.gov, formerly irbis.llnl.gov. Use FTP to access it either by name or IP address (128.115.19.53). The operation and prompt will depend on which vendor's FTP you are running. Usually, you must first log in before you can list directory contents and transfer files. Use "ftp" or "anonymous" for Name or Foreign username unless given a general prompt such as ciac.llnl.gov> or ftp>. In that case, enter the keyword "user" or "login" before "ftp" or "anonymous" (e.g. user ftp). Use your Internet E-mail address for the Password.

Once logged in you may type a question mark to find out what key-words are recognized. The file 0-index.txt (in the top level directory /ftp) is a document explaining the directory structure for downloadable files. The file whatsnew.txt (in directory /ftp/pub/ciac) contains a list of the new files placed in the archive. Use the command *get* [for single files] or *mget* [for multiple files] to download one or more files to your own machine.

Publications Available from CIAC

CIAC prepares publications on a variety of computer security related topics, the CIAC 2300 series. Many of these will be updated as needed to keep the information current. We welcome suggestions for topics that you feel would be valuable. We also make available some documents from other sources. In the table below, column **E** is for electronic documents available via CIAC's servers (see above article). Column **P** is for printed documents, for those who do not have Internet or telephone-modem access. The electronic formats are: *.txt for ASCII, *.ps for PostScript™, *.hqx for bin-hexed Microsoft Word, *.wp5 for PC Word Perfect v 5.0.

No.	E	P	TITLE
2300	x	x	Abstracts of the CIAC-2300 Series Documents
2301	x	x	Computer Virus Information Update
2302	x	x	The FELICIA Bulletin Board System and the IRBIS Anonymous FTP Server
2303	x	x	The Console Password Feature for DEC Workstations
CIAC	x		Incident Handling Guidelines
LLNL	x		User Accountability Statement, E. Eugene Schultz, Jr.
SRI	x		Improving the Security of your Unix System, David A. Curry
LLNL	x		Incident Handling Primer, Russell L. Brand
ORNL	x		Terminal Servers and Network Security, Curtis E. Bemis & Lynn Hyman

To obtain further information, contact Allan L. Van Lehn, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

Who is CIAC

CIAC is the United States Department of Energy's Computer Incident Advisory Capability. We provide incident handling assistance, computer security training and awareness activities, and related services. The following people are presently assigned to the CIAC Team. Each has varied computer security experience and specializations. Sandra L. Sparks is the CIAC Project Leader. Sandy is available to talk with you via phone at 510-422-6856 or E-mail as ssparks@llnl.gov. In an emergency incident situation, she can be contacted via the secondary skypage: call 1-800-SKYPAGE (759-7243) and enter PIN number 8550074.

Name	Technical Support Areas
Sandy Sparks	Unclassified computer security, ibm vm/cms
Rich Feingold	Training, openvms, ultrix, unix, pc's, networks
Bill Orvis	Viruses, pc's, hardware, unix
Karyn Pichnarczyk	Viruses, pc's, unix
Sandy Sydnor	Administrative support coordinator
Allan Van Lehn	OpenVMS, sys admin, publications, unix, pc's
Steve Weeber	SunOS, unix, x-windows, firewalls, networks

To obtain further information contact, Allan L. Van Lehn, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

Contacting CIAC

If you require additional assistance or wish to report a vulnerability, call CIAC at 510-422-8193, fax messages to 510-423-8002 or send E-mail to ciac@llnl.gov. For emergencies and off-hour assistance, call 1-800-SKY-PAGE (759-7243) and enter PIN number 8550070 (primary) or 8550074 (secondary). The CIAC Duty Officer, a rotating responsibility, carries the primary skypager. The Project Leader carries the secondary skypager. If you are unable to contact CIAC via phone, please use the skypage system.

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.

End of CIAC Notes Number 94-03a 94_07_06