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-SKYPAGE (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.

End of CIAC Notes Number 02e 94_05_12

SPI-ANNOUNCE and SPI-NOTES. The SPI-ANNOUNCE list will be used by the SPI team to provide official news about SPI software updates, new features, and general information regarding SPI distribution availability. The second list, SPI-NOTES, is an unmoderated forum for users to discuss problems and solutions regarding the use of SPI products. To subscribe to one of these mailing lists, in the body of the message substitute SPI-ANNOUNCE or SPI-NOTES for *list-name* and valid information for *LastName, FirstName* and *PhoneNumber* when sending

E-mail to `ciac-listproc@llnl.gov`

```
      subscribe  list-name   LastName, FirstName  PhoneNumber
e.g., subscribe spi-announce Butler, Rhett G. 404-555-1212 x42
```

You will receive an acknowledgment containing address, initial PIN, and information about how to change either of them, cancel your subscription, or get help.

PLEASE NOTE: The RETURN ADDRESS of the E-mail you send is used by ciac-listproc to identify incoming requests. Mail from a new address will be rejected until you send a "set" command changing your subscription address. You may use this address change to subscribe a distribution-list address to the SPI-ANNOUNCE service, rather than have each of the recipients subscribe to the service individually. If you have any questions about this list, you may contact the list's owner: listmanager@cheetah.llnl.gov.

CIAC Publications

CIAC is preparing publications on a variety of computer security related topics. Many of these will be updated as needed to keep the information current. The publications will be available in electronic form via CIAC's servers or in printed form for those who do not have Internet or telephone-modem access. We welcome suggestions for topics that you feel would be valuable. The publications available are:

CIAC #	TITLE
2300	Abstracts of the CIAC-2300 Series Documents
2301	Computer Virus Information Update
2302	The FELICIA Bulletin Board System and the IRBIS Anonymous FTP Server
2303	The Console Password Feature for DEC Workstations

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	IBM VM/CMS, PC systems
Rich Feingold	OpenVMS, ULTRIX, Unix, PC, networks, training
Bill Orvis (half time)	DOS, Macintosh, UNICOS, OpenVMS, engineering
Karyn Pichnarczyk	DOS, Macintosh, viruses, Unix
Sandy Sydnor	Administrative support coordinator
Allan Van Lehn	OpenVMS, sys admin, special projects, Publications
Steve Weeber	SunOS, Unix, X-windows, firewalls, Netmap

E-14 Advisory	wuarchive ftpd Trojan Horse Some copies of the wuarchive FTP daemon before version 2.3 have been modified to contain a Trojan Horse.	April 6, 1994, 1640 PDT
E-15a Bulletin	*Restricted Distribution*	April 7, 1994 0930 PDT
E-16a Bulletin	*Restricted Distribution*	April 7, 1994 1000 PDT
E-17 Bulletin	FTP Daemon Vulnerabilities There are active expolitations of several implementations of the FTP daemon. Immediate upgrade recommended	April 14, 1994 1130 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*.;

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:;*

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.

Security Profile Inspector Mailing List

The Security Profile Inspector (SPI) Development team has established two self-subscribing E-mail lists to service the SPI user community. These lists are titled

An unexpected system conflict sometimes results in Disinfectant 3.4 giving the "unexpected error -192" message when running on Macs with enabler versions 003 (the LC III) and 040 (the Centris/Quadra 610, 650, and 800), and with the 32 bit system enabler. You can safely ignore this error message as it does not signify a real problem. Disinfectant 3.4 and the Disinfectant INIT can both be safely used on all Macintosh systems to protect against all known Macintosh viruses. John Norstad, the author of Disinfectant, released version 3.4.1 to fix this bug. It has been announced and made available in all the usual places, e.g., ftp.acns.nwu.edu, sumex-aim.stanford.edu, AppleLink, rascal.ics.utexas.edu, America Online, CompuServe, Genie, Calvacom, MacNet, Delphi, and comp.binaries.mac.

CIAC would like to thank Gene Spafford of Purdue University for releasing the information about this virus.

To obtain further information, contact Karyn Pichnarczyk, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

CIAC Info Articles

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 to close, potentially or actively exploited vulnerabilities. Advisory notices are delivered as quickly as possible via FAX, E-mail, and postal service.

E-07 Bulletin	Unix sendmail Vulnerabilities Update Gives status of vendor security patches to correct vulnerabilities in the Unix sendmail utility (see CIAC Advisory E-03). Workarounds given in E-03 may be safely used even after vendor patches have been installed.	January 7, 1994, 0900 PST
E-08 Bulletin	*Restricted Distribution*	January 25, 1994, 1530 PST
E-09 Advisory	Network Monitoring Attacks Unauthorized access and use of resources; exposure of username, password, host-name combinations, as well as other sensitive information.	February 3, 1994, 2130 PST
E-10 Bulletin	IBM AIX Performance Tools Vulnerability Unprivileged local users may gain unauthorized root access.	February 24, 1994, 2000 PST
E-11 Bulletin	Lotus cc:Mail Security Upgrade Available Accounts could be compromised if another person is allowed access to a cc:Mail user's personal computer	March 7, 1994, 0900 PST
E-12 Advisory	Network Monitoring Attacks Update New information on the problem, actions to take to eliminate vulnerabilities and strengthen system security. Tables of checksums for many SunOS files and patches	March 18, 1994 1800 PST
E-13 Advisory	Sun Announces Patches for /etc/utmp Vulnerability SunOS 4.1.x systems (but not SunOS 4.1.3_U1 or Solaris 2.x) systems need to patch dump, in.comsat, in.talkd, shutdown, syslogd, and write.	March 21, 1994, 1200 PST

MAC User Articles

Current Macintosh Anti-Virus Software

Reference to any specific commercial product does not necessarily constitute or imply its endorsement, recommendation or favoring by CIAC, the United States Government or the University of California. As of March 9, 1994, the current versions of Macintosh anti-virus software [all released early March, 1994] are:

Product Name	Version	Comments
CPAV	3.0c	Central Point Software Inc. BBS: 503-690-6650 New 'MacSig' antidote file available dated 3/4/94
Disinfectant	3.4.1	Free Software. Version 3.4 was released to find the INIT-9403 virus, a small bug was found, so 3.4.1 was released
Gatekeeper	1.3.1	Free Software. There are as-yet (3/8/94) unanswered questions whether the old version 1.3 is able to locate INIT-9403
Rival	INIT-9403 Vaccine	E-mailed to all registered users. Contact authors if you haven't upgraded to 1.2.5 yet. Otherwise, the vaccine will be sent to your account.
SAM Virus Clinic & Intercept	3.5.11	Symantec Customer Service 800-441-7234
Virex	5.02	Datawatch Corp., Triangle Sw. Div. 919-549-0711, BBS: 919-549-0042
VirusDetective	5.0.11	Shareware (product phasing out). Search strings will be sent to registered users only

To obtain further information, contact Karyn Pichnarczyk, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

New Macintosh Virus: INIT-9403

The discovery of a new Macintosh virus was announced March 3rd, 1994. This virus, the INIT-9403 Virus, is a malicious virus which will erase disk information on all connected hard drives, as well as erase the boot volume after a preset number of files have been infected.

The virus initially infects by altering the Finder file, then may insert copies of itself in various compaction, compression, and archive programs (programs most likely to be shared with other Macintoshes). This virus has only been seen on Italian systems, so far. If you detect this virus on a non-Italian system, please contact CIAC immediately.

New releases of anti-virus software for the Macintosh detect and eradicate this virus.

At least one vendor has decided to call the INIT-9403 virus the "SysX" virus. Since there is no common naming scheme for new Mac viruses, expect to see the names "INIT-9403" and "SysX" and as aliases.

Lotus cc:Mail Caution

CIAC recently released CIAC Bulletin E-11, Lotus cc:Mail Security Upgrade Available. In response to that bulletin, CIAC received the following information about a function in cc:Mail that has security implications.

The following three lines may be visible in your CONFIG.SYS file:

SET CCNAME=Your Name
SET CCPASSWORD = Your Password
SET CPATH=Your Post Office path name

The "Your Password" field will be visible in plain text. CIAC has contacted Lotus about this vulnerability, and they have answered that this information will *only* be placed at the end of a user's CONFIG.SYS file if the user selects the automatic login option at cc:Mail installation.

CIAC strongly recommends that this automatic login option NOT be selected. To determine if your system has been set up in this manner, type out your CONFIG.SYS file. If the SET CCPASSWORD line is present, simply edit the line out of the file using any file editor. Once edited out of the file, the system will prompt you for a password at each login.

CIAC would like to thank Tom Obenauf of Sandia National Laboratories for bringing this to our attention.

To obtain further information, contact Karyn Pichnarczyk, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

* Note: The Department of Energy has a site license for Data Physician Plus. It is available from your site CPPM.

To obtain further information, contact Karyn Pichnarczyk, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

Maltese Amoeba False Positive Detection - PKZIP

Version 2.04C of PKZIP, the popular file compression utility is known to cause false positive detection of the Maltese Amoeba Virus by several popular anti-virus scanners. The current versions of anti-virus scanners have been updated to correct this problem, and PKZIP has been updated to version 2.04D, which does not cause a positive detection by old versions of the scanners. If you have a detection of the Maltese Amoeba in PKUNZIP.EXE, and it came from version 2.04C (PKZ204C.EXE), and you are using an old version of an anti-virus scanner, then you probably don't have a virus infection. However, you should still treat it as a virus infection until you can scan the program with a newer version of your virus scanner.

To obtain further information, contact William J. Orvis, CIAC, 510-422-8193 or send E-mail to ciac@llnl.gov.

Math Co-processor Problem

CIAC received information from Pacific Northwest Laboratory about the following problem and fix. There is a potential problem with floating point calculations, recently discovered on the following systems:

- Zeos 486DX with the Award BIOS v3.1, revisions 452-0005-02A and 452-0005-01B and Gateway 486DX machines with Phoenix BIOS 0.10 G14.
- IBM 486DX Valuepoint (not enough information available yet as to particular BIOS revisions or models).
- A couple no-name brands (seriously, there was no identification on the case) with 386DX processors and 80387 co-processors and the American Megatrends BIOS.

In particular, several configurations were found that improperly report the results of a "divide by zero" floating point operation.

NOTE: It is not known if the problem is restricted to these particular machines or whether it is a configuration issue on these machines.

Examples of applications which use floating point operations are CAD/CAM, custom developed and statistical applications. The impact on floating point operations by EXCEL and other office automation applications is being checked.

Procedures for checking a standalone system for the floating point "divide by zero":

1) Place a copy of FPTEST.EXE and DIVZERO.EXE on a floppy.
2) Restart the computer you want to test by rebooting.
3) Place the floppy in drive A or B.
2) Change to that drive.
3) Type at the A:> (or whatever drive you are at) FPTEST -D.

The program will tell you it is testing the math co-processor and whether or not it passes the test. The programs, FPTEST.EXE and DIVZERO.EXE, are now available to DOE sites via anonymous ftp from ftp.pnl.gov in the directory /pub/outgoing (files will be deleted automatically in seven calendar days). Non-DOE sites wanting anonymous access to ftp.pnl.gov should mail a request to ftpadmin@ftp.pnl.gov.

The security of each system can be greatly enhanced by requiring one-time passwords, installing software that limits system access (e.g., TCP wrapper), a monitor for unauthorized system changes (e.g., SPI) and a monitor for intrusions (e.g., NID). Please see the above feature article “Available Security Tools for Unix and Other Systems” for availability information.

DEC User Articles

OpenVMS Security Update Patch Kits

Digital Equipment Corporation has developed OpenVMS VAX and Alpha AXP patch kits for their software warranty and software contract maintenance customers. The kit for OpenVMS VAX versions 5.4-3, 5.5, 5.5-1, 5.5-2, 5.5-2H4, 5.5-2HF, and 6.0 began to ship mid-March. The kit for OpenVMS AXP versions 1.5 and 1.5-1H1 shipped in January ‘94. These kits contain a large number of patches available from Digital. The kits make it easy to install this collection of remedial fixes, thus helping those running older versions. A few of the patches provide enhanced security, hence the designation “security kit.” Future releases of OpenVMS will incorporate these patches.

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

PC User Articles

Current PC Anti-Virus Software

Reference to any specific commercial product does not necessarily constitute or imply its endorsement, recommendation or favoring by CIAC, the United States Government or the University of California. As of March 10, 1994, the current versions of PC anti-virus software are:

Product Name	Company	Version	Date released
AVP	Kami Limited	1.07	October 1993 with 1/94 update
CP AntiVirus (CPAV)	Central Point Software Inc.	2.1	November 1993
Data Physician PLUS! *	Digital Dispatch Inc.	4.0C	January 1994
FindVirus - Dr.Solomon’s AntiVirus Toolkit	Ontrack Computer Systems Inc.	FV 6.54	March 1994
F-PROT	FRISK Associates	2.11	February 1994
IBM Antivirus	IBM Corp.	1.05	February 1994
Integrity Master	Stiller Research, Dept. B1	2.21	February 1994
Norton AntiVirus (NAV)	Symantec Corp.	3.0.2	December 1993
PC Rx Antivirus	Trend Micro Devices Inc.	2.65	?
SCAN	McAfee Associates	921v111	January 1994
Thunderbyte (TBAV)	?	6.10	January 1994
Untouchable	Fifth Generation Systems Inc.	29.04	?
VET	Cybec	7.52	November 1993
Virex for the PC	Datawatch, Triangle Sw. Div.	2.93	February 1994
ViruSafe	EliaShim Microcomputers Inc.	5.3	?
VirusBuster	Thompson Network Security	3.98	?

Upcoming computer security related conferences

DOE's Computer Security Training Conference
May 2-5, 1994
Sheraton Denver Tech Center Hotel, Denver, Colorado
Who to contract: DOE CSG Training (301) 903-4195
Ms. Eunice Warmoth, Conference Chair, EG&G Mound Applied Technologies
Dr. Rowena Chester, Program Chair, Martin Marietta Energy Systems
Conference Registration must be received by April 22, 1994.

This is a forum for DOE and DOE contractor personnel to share computer security information and concerns. Five parallel workshop sessions will be offered. Technical sessions are divided into three tracks: technical, management, and general. A computer security video session and some "birds of a feather" technical sessions are also planned.

Sixth Annual Computer Security Incident Handling Workshop
hosted by FIRST
July 25-29, 1994
Boston, Massachusetts

This annual Incident Handling Workshop is part of FIRST's ongoing program of education and awareness for its members and others. The workshop is targeted at the growing number of computer security professionals who must deal with increasingly sophisticated security incidents and system vulnerabilities. The focus of this year's three day 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. The presentations will focus on tools that are utilized in incident handling such as: intrusion/vulnerability detection tools, system/network monitoring tools, informational resources, legal and administrative issues in incident handling for international incidents, incident handling and the National Information Infrastructure

If you have questions regarding this year's event, please direct them to:
FIRST Secretariat: workshop-info@first.org

Unix User Articles

Network Sniffer Attacks Continue

The magnitude of this problem continues to be revealed by discovery of more Internet monitoring attacks affecting additional systems and sites. CIAC urges all Unix System Administrators to take steps to learn about the nature of these attacks and employ the countermeasures needed. Please refer to CIAC Advisories E-09, E-12, and E-13. Advisory E-12 has a lengthy listing of cryptographic checksums and a tool to automate system inspection. As corrected or new information comes to our attention, we are updating the list used by this tool. The most current data will be available via anonymous ftp from irbis.llnl.gov in the directory /pub/util/crypto/md5_sun.v(1, 2, ... etc.).

System administrators must check all Unix systems to ensure that no Trojan horse files have replaced system utilities and libraries. If the system is "clean," then all known security patches must be installed. If the system is compromised, a complete backup should be done, a "clean" system must be installed. New passwords must be required for all accounts, and hidden logs of sniffed accounts and passwords found. All logs should be searched for evidence of other compromised systems.

4. Encryption/Authentication Tools

Tool: DES - KA9Q
Description: A U.S. written implementation of DES is part of the KA9Q packet radio implementation. This version is not exportable.
Availability: anonymous ftp from ucsd.edu:/hamradio/packet/tcpip/crypto/des.tar.Z

Tool: DES
Description: An implementation of DES suitable for use with Kerberos and compatible with DES packages offered by several Unix vendors. Because this implementation was not created in the U.S., export restrictions do not apply.
Availability: anonymous ftp from kampi.hut.fi

Unix Tool: MD4 / MD5
Description: MD4 is another message-digest function proposed by Ron Rivest, similar to SNEFRU but implemented differently, produces a fixed 128 bit output. MD5 is newer and slightly more secure in the face of certain cryptographic attacks.
Availability: anonymous ftp from rsa.com

Tool: kerberos
Description: Kerberos is a DES-based encryption scheme that encrypts sensitive information, such as passwords, sent via the network from client software to the server daemon process. The network services will automatically make requests to the Kerberos server for permission "tickets." You will need to have the source to your client/server programs so that you can use the Kerberos libraries to build new applications.
Availability: anonymous ftp from athena-dist.mit.edu

Tool: S/Key™
Description: Bellcore developed S/Key™, a one-time password system providing authentication over networks that are subject to eavesdropping/replay attacks. The user's secret password never crosses the network during login, or when executing other commands requiring authentication. No secret information is stored anywhere, and the algorithm is public knowledge. The remote (client) end of this system can be run on any computer. The host (server) end can be integrated into any application requiring authentication. A prototype system has been built for a Unix, MAC, and PC environment, but there is nothing Unix-specific about the design.
Availability: anonymous ftp from thumper.bellcore.com/pub/skey

Unix Tool:	securelib
Description:	SecureLib contains replacement routines for three SunOS kernel calls: accept(), recvfrom(), recvmsg(). These replacements, compatible with the originals, add functionality to check the Internet address of the machine initiating the connection makeing sure that it is <u>allowed</u>. A configuration file defines what hosts are allowed for a given program. Once these replacement routines are compiled, they can be used when building a new shared libc library. The resulting "libc.so" can then be put in a special place. Any program that should be protected can then be started with an alternate LD_LIBRARY_PATH.
Availability:	anonymous ftp from eecs.nwu.edu

Unix Tool:	socks
Description:	"Sockd" and the "Socks Library" provide another way to implement a "TCP Wrapper." It is not intended to make the system it runs on secure, but rather to centralize (<u>firewall</u>) all external Internet services. The sockd process is started by inetd whenever a connection is requested for certain services. Then it allows connections only from approved hosts (listed in a configuration file). Sockd also will log information about the connection. You can use the Socks Library to modify the client software to directly utilize sockd for outgoing connections. This is very tedious and requires you to have client program source code.
Availability:	anonymous ftp from s1.gov

Unix Tool:	npasswd
Description:	Like passwd+, npasswd is a replacement for the standard "passwd" command that prevents users from selecting easily-guessable passwords.
Availability:	anonymous ftp from emx.utexas.edu

Unix Tool:	Tripwire
Description:	Tripwire is an integrity-monitor for Unix systems. It uses checksums and message digests to build a list of *signatures* for monitored files, and can be rerun to check for changes. It can monitor selected items of system-maintained information, changes in permissions, links, sizes of directories and files, and additions or deletions of files from watched directories. It should work on almost any version of Unix, makes no changes to system files and does not require root privilege to run. It is distributed as papers and source code.
Availability:	anonymous ftp from ftp.cs.purdue.edu/pubs/spaf/COAST/Tripwire or WWW http from www.cs.purdue.edu/homes/spaf/coast.html

Unix Toolkit:	CrackLib
Description:	CrackLib is a library of C functions to be used in your own password checking program. Prevents users from choosing passwords that could be guessed by CRACK. *Note well:* CrackLib is <u>not</u> a replacement "passwd" program. CrackLib is a *library*. You must add it into your own "passwd" program (if you have source code) or to "shadow" (off of the net).
Availability:	anonymous ftp (CrackLib + large dictionary) from black.ox.ac.uk:~ftp/src/security/cracklib25.tar.Z

Unix Tool: COPS (Computer Oracle and Password System)
Description: A collection of programs that each attempt to tackle a different problem area of Unix security. Following is a list of the areas checked:

- file, directory, and device permissions/modes
- poor passwords
- content, format, and security of password and group files
- the programs and files run in /etc/rc* and cron(tab) files
- existence of root-SUID files
- a CRC check against important binaries or key files
- writability of users home directories and startup files (.profile, .cshrc, etc.)
- anonymous ftp setup
- unrestricted tftp, decode alias in sendmail, SUID uudecode problems, hidden shells inside inetd.conf, rexd running in inetd.conf
- miscellaneous root checks

Availability: anonymous ftp from cert.org

Unix Tool: CRACK
Description: CRACK is a fast Unix password cracking program designed to assist site administrators in ensuring effective password use. It is approximately eight times faster than standard DES routines, enabling one to check more passwords in a given time. CRACK is widely available and presumed to be used by intruders.
Availability: anonymous ftp from cert.org

Unix Tool: TAMU Suite of Tools
Description: This package includes three coordinated sets of tools: “drawbridge,” a powerful bridge filtering package; “tiger,” a set of machine checking programs; and “netlog”, a set of intrusion detection, network monitoring programs.
Availability: anonymous ftp from sc.tamu.edu

3. Security Enhancement Tools

Unix Tool: TCP Wrapper
Description: With this package you can monitor incoming connections to the SYSTAT, FINGER, FTP, TELNET, RLOGIN, RSH, EXEC, TFTP, TALK, and other IP network utilities. Connections are reported through the syslog daemon. Requirements are that network daemons are started by the inetd program or something similar, and the availability of a syslog(3) library. Optional features are: access controls to limit the number of hosts that can connect to your network daemons, remote user name lookups with the RFC 931 protocol, and protection against hosts that pretend to have someone else’s host name.
Availability: anonymous ftp from ftp.win.tue.nl

Unix Tool: passwd+
Description: Passwd+ is a proactive password checker that replaces /bin/passwd on your system. It is rule-based and easily configurable. It prevents users from selecting a weak password so that programs like CRACK can’t guess it, and it provides enhanced syslog logging.
Availability: anonymous ftp from dartmouth.edu

1. Tracing/Tracking Tools

Tool: NID (Network Intrusion Detector)
Description: NID is an Ethernet Monitoring tool that checks packet streams for known suspicious security activities. Session isolation and replay capabilities are offered.
Availability: While not available to the general public, it is available free of charge to all U.S. Department of Energy sites and contractors. Send E-mail to ciac@llnl.gov. It is also available to all U.S. Department of Defense organizations via DISA's ASSIST Team. Send E-mail to assist@assist.ims.disa.mil.

Unix Tool: traceroute
Description: For tracing routes between the current host and other Internet sites. Useful for examining hops, detecting sites that are down, or sites that do not resolve properly.
Availability: in comp.sources.unix archives, ftp from many sites including ftp.uu.net

Unix Tool: tcpdump
Description: For monitoring TCP/IP packets for BSD-based Unix systems.
Availability: anonymous ftp from ftp.ee.lbl.gov

Unix Tool: dig
Description: For querying Domain Name Service servers in a more flexible, convenient manner than nslookup.
Availability: anonymous ftp from venera.isi.edu

2. Security Assessment Tools

OpenVMS Tool: SPI/VMS (Security Profile Inspector for OpenVMS)
Description: SPI/VMS is an administrator's tool that checks configuration options, includes a file-change (integrity) checker to monitor for backdoors and alteration of identified files, and various other security checks.
Availability: While not available to the general public, it is available free of charge to all U.S. Department of Energy sites and contractors. Send E-mail to ciac@llnl.gov. It is also available to all U.S. Department of Defense organizations via DISA's ASSIST Team. Send E-mail to assist@assist.ims.disa.mil.

Unix Tool: SPI/Unix (Security Profile Inspector for Unix)
Description: SPI/Unix is a screen-based administrator's tool that, which is a superset of COPS, checks configuration options, includes a file-change (integrity) checker to monitor for backdoors and viruses, and various other security checks.
Availability: While not available to the general public, it is available free of charge to all U.S. Department of Energy sites and contractors. Send E-mail to ciac@llnl.gov. It is also available to all U.S. Department of Defense organizations via DISA's ASSIST Team. Send E-mail to assist@assist.ims.disa.mil.

Feature Articles

FIRST the Forum of Incident Response and Security Teams

CIAC is a member of FIRST. This group includes response teams from the U.S. government such as the DoD's ASSIST and NASA's NASIRC; university teams such as CERT/cc; international teams such as CERT-NL in the Netherlands; and commercial teams such as Apple's APPLECORE group. FIRST members work together handling major incidents and sharing information needed to combat hacker-intruders and system vulnerabilities. Much of the administrative support for FIRST comes from NIST, the National Institute for Standards and Technology which maintains FIRST mailing lists, document servers, etc. A list of FIRST member organizations and their constituencies can be obtained by sending E-mail to first-request@first.org with an empty subject line and a message body containing the line: send first-contacts. Information about FIRST can be obtained by sending E-mail to first-request@first.org with an empty subject line and a message body containing the line: send info. Information about FIRST's Annual Computer Security Incident Handling Workshops can be obtained by sending E-mail to workshop-info@first.org with an empty subject line and a message body containing the line: send info.

The following feature article on available security tools is based on information collected by FIRST. The sections on CrackLib, NID, SPI, S/Key™ and Tripwire have been added or revised.

Available Security Tools for Unix and Other Systems

Of the many tools available for system and network security, a number are useful in incident handling. This article provides access information for a subset of tools considered most useful for incident handling. The tools are divided into four categories:

1 - tracing and tracking tools - for tracing connections and examining raw TCP/IP data.
2 - security assessment tools - for examining host security, passwords, and configuration.
3 - security enhancement - for improving host security.
4 - encryption - useful utilities for storing and exchanging encrypted data. NIST has released a Federal Information Processing Standard (FIPS) allowing software implementation of DES. Several are listed.

Active use of these tools can enhance security, prevent break-ins, or help you determine if your system has been compromised. The vast majority of these tools are for Unix and all have something to do with the Internet and the TCP/IP protocol suite. If you recommend other tools, please contact CIAC.

To obtain up-to-date, tools-related information, you can subscribe to the following E-mail lists and news groups:

cert-tools - send E-mail to cert-tools-request@cert.org
comp.security.misc
sci.crypt
comp.sources.binaries

U.S. DOE's Computer Incident Advisory Capability

CIAC NOTES

Number 02e May 12, 1994

Recently some DOE sites have needed to contact CIAC during off hours. 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 second issue of CIAC Notes! CIAC has experienced its busiest three months since the Internet Morris Worm attack November 2, 1988. Recent headlines such as "Security Breach at the Internet Raises Worries" barely exposes the potential consequences of the recent Internet attacks. Of the estimated hundred thousand of IDs and passwords captured by unauthorized personnel, some are DOE related. As long as login passwords must travel in plain text over our networks, DOE and other organizations connected to the Internet must give serious consideration to using one-time passwords. S/Key™ is a Bellcore developed, one-time password implementation available via anonymous ftp from thumper.bellcore.com. Additional sources of information and tools that can help security professionals respond to the present Internet Attack are included in the feature articles and in the Unix user section of this issue.

In future issues, CIAC plans articles on one-time passwords and the security concerns around E-mail, gopher and mosaic. If you have topics you would like CIAC to address 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.

Table of Contents