CERT:
explained

The CERT* Coordination Center FAQ

==========
= Preface =
==========

This document is intended to answer the most Frequently Asked Questions (FAQs) about the CERT Coordination Center. The FAQ is a dynamic document that will change as information changes. Suggestions for additional sections are welcome -- please e-mail them to cert@cert.org. The most recent copy of this FAQ will be available via anonymous FTP from info.cert.org in the /pub directory.

Questions answered in this document

==========

= Section A. Introduction to the CERT Coordination Center =

==========

A1. What is the CERT Coordination Center?

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

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

A2. CERT Coordination Center contact information:

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

Internet E-mail address
cert@cert.org

Telephone number
+1 412-268-7090 (24-hour hotline)
CERT Coordination Center personnel answer
8:30 a.m.- 5:00 p.m. EST(GMT-5)/EDT(GMT-4), on call for emergencies during other hours.

FAX number
+1 412-268-6989

A3. What's in the CERT name?

Since its beginning in 1988, the CERT Coordination Center has acquired its name through an evolutionary process. Because of this, you may see the CERT Coordination Center referred to by several different names. While you may hear us called Computer Emergency Response Team, CERT/CC, or CERT, our proper name is the CERT Coordination Center.

CERT(sm) is a service mark of Carnegie Mellon University.

The CERT e-mail address has undergone a similar evolution. We use the e-mail address:

cert@cert.org

Any references to:

cert@cert.sei.cmu.edu
or
cert@sei.cmu.edu

should be changed to the new address (cert@cert.org).

==========

= Section B. Where To Go for Information =

==========

B1. What is a CERT advisory?

A CERT advisory provides information on how to obtain a patch or

details of a workaround for a known computer security problem. The CERT Coordination Center works with vendors to produce a workaround or a patch for a problem, and does not publish vulnerability information until a workaround or a patch is available. A CERT advisory may also be a warning to our constituency about ongoing attacks (e.g., "CA-91:18.Active.Internet.tftp.Attacks").

CERT advisories are published on the USENET newsgroup:

comp.security.announce

and are distributed via the cert-advisory mailing list. Both of these publication methods are described below.

CERT advisory archives are available via anonymous FTP from info.cert.org in the /pub/cert_advisories directory.

B2. Where can I obtain archived CERT advisories?

CERT advisories are available via anonymous FTP from info.cert.org in the /pub/cert_advisories directory. The "01-README" file provides a short summary of each of the advisories.

B3. Can I get source code to a patch described in a CERT advisory?

The CERT Coordination Center does not provide source-level patches. Some vendors make source-level patches available to their source customers while others only distribute binary patches. Contact your vendor for more information.

B4. What security mailing lists, newsgroups, and other sources of information does the CERT Coordination Center recommend?

(a) CERT mailing lists

(1) CERT advisory mailing list

The CERT Coordination Center maintains a CERT advisory mailing list for those members of the

constituency who are unable to access USENET news or who would like to have advisories mailed directly to them or to a mail exploder at their site. If you would like to be added to the mailing list, please send mail to:

cert-advisory-request@cert.org

You will receive confirmation mail when you have been placed on the list.

(2) CERT tools mailing list

The purpose of this moderated mailing list is to encourage the exchange of information on security tools and techniques. The list should not be used for security problem reports.

The CERT Coordination Center will not formally review, evaluate, or endorse the tools and techniques described. The decision to use the tools and techniques described is the responsibility of each user or organization, and we encourage each organization to thoroughly evaluate new tools and techniques before installation or use.

Membership is restricted to system programmers, system administrators, and others with a legitimate interest in the development of computer security tools. If you would like to be considered for inclusion, please send mail to:

cert-tools-request@cert.org

You will receive confirmation mail when you have been placed on the list.

(b) Other security-related mailing lists

(1) VIRUS-L mailing list (see comp.virus newsgroup below)

VIRUS-L is a moderated mailing list with a focus on computer virus issues. For more information, including a copy of the posting guidelines, see the file "virus-l.README", available by anonymous FTP from cs.ucr.edu. To be added to the mailing list, send mail to:

listserv@lehigh.edu

In the body of the message, put nothing more than:

SUB VIRUS-L your name

(2) Firewalls mailing list

The Firewalls mailing list is a discussion forum for firewall administrators and implementors. To subscribe to Firewalls, send mail to:

Majordomo@GreatCircle.COM

In the body of the message, put only:

subscribe firewalls

(3) Firewalls digest

The Firewalls digest is a compilation of messages from the Firewalls mailing list. To subscribe to the Firewalls digest, send mail to:

Majordomo@GreatCircle.COM

In the body of the message, put only:

subscribe firewalls-digest

Compressed back issues are available via anonymous FTP

from:

FTP.GreatCircle.COM

in pub/firewalls/digest/vNN.nMMM.Z (where "NN" is the volume number and "MMM" is the issue number).

(c) USENET newsgroups

(1) comp.security.announce

The comp.security.announce newsgroup is moderated and is used solely for the distribution of CERT advisories.

(2) comp.security.misc

The comp.security.misc is a forum for the discussion of computer security, especially as it relates to the UNIX(r) Operating System.

(3) alt.security

The alt.security newsgroup is also a forum for the discussion of computer security, as well as other issues such as car locks and alarm systems.

(4) comp.virus

The comp.virus newsgroup is a moderated newsgroup with a focus on computer virus issues. For more information, including a copy of the posting guidelines, see the file "virus-l.README", available via anonymous FTP on info.cert.org in the /pub/virus-l directory.

(5) comp.risks

The comp.risks newsgroup is a moderated forum on the risks to the public in computers and related systems.

(d) NIST (National Institute of Standards and Technology)
Computer Security Bulletin Board

Information posted on the bboard includes an events calendar, software reviews, publications, bibliographies, lists of organizations, and other government bulletin board numbers. This bboard contains no sensitive (unclassified or classified) information.

If you have any questions, contact NIST by phone at: 301-975-3359; by FAX at: 301-590-0932; or by e-mail at: csrc@csrc.ncsl.nist.gov.

B5. What information is available via anonymous FTP from CERT?

The CERT Coordination Center has a variety of computer security information available by anonymous FTP to info.cert.org in /pub directory. In the /pub directory, the file "ls-lR" lists the subdirectories and the files found in those subdirectories. Examples of what you will find in the /pub directory are listed below.

/pub/CERT_Press_Release_8812: The file "CERT_Press_Release_8812" is a copy of the December 1988 DARPA press release announcing the formation of the CERT Coordination Center.

/pub/FIRST: The /pub/FIRST directory contains a file, "first-contacts". FIRST, the Forum of Incident Response and Security Teams, is an organization whose members work together voluntarily to deal with computer security problems and their prevention. General information on FIRST is available via anonymous FTP from csrc.ncsl.nist.gov in the /pub/first directory. The name of the file is "op_frame.txt". The document begins with a description of the CERT System, which was later renamed "FIRST". Also in that directory are the minutes from meetings, a list of FIRST contacts (also duplicated in the CERT anonymous FTP area on info.cert.org in the /pub/FIRST directory), and other related

information.

/pub/cert_advisories: The /pub/cert_advisories directory contains archived copies of past CERT advisories, the "01-README" file, a copy of the CERT press release from December 1988 announcing the formation of the CERT Coordination Center, an article from the March 1990 issue of Bridge, a magazine published by the Software Engineering Institute (SEI), describing CERT, and a file containing information on the status of the rdist patch.

/pub/clippings: The /pub/clippings directory is an archive service for computer security. This archive is a central repository for selected security related USENET News and mailing list postings. The archive will not be restricted to any one newsgroup or mailing list. To submit an article for the clippings archive, please send e-mail to:

clip@cert.org

/pub/cops: The /pub/cops directory includes the information for the COPS package. COPS is a publicly available collection of programs that attempts to identify security problems in the UNIX Operating System. COPS does not attempt to correct any discrepancies found; it simply produces a report of its findings.

/pub/info: The /pub/info directory contains online copies of security-related books and papers, including Dave Curry's May 1990 SRI Tech Report "Improving the Security of Your Unix System", "Computer Emergency Response - An International Problem" by Richard D. Pethia and Kenneth R. van Wyk, the report "Coping with the Threat of Computer Security Incidents: A Primer from Prevention through Recovery" by Russell Brand, and the Department of Defense Trusted Computer System Evaluation Criteria CSC-STD-001-83 often referred to as the "Orange Book". (Note: This is the Aug 1983 version of this document; this document was revised in Dec 1985.)

/pub/network_tools: The /pub/network_tools directory contains network tools made available via anonymous FTP. The file

"tcp_wrapper.xx" is a TCP daemon wrapper program that will provide additional logging information and access control for many network services (also duplicated in the /pub/tools directory).

/pub/papers: The /pub/papers directory contains the announcement of the CERT tools mailing list.

/pub/ssphwg: The /pub/ssphwg directory contains archived information from the IETF Site Security Policy Handbook Working Group and the IETF Security Policy Working Group. RFC 1244, "Site Security Handbook" was the result of the Site Security Policy Handbook Working Group; and RFC 1281, "Guidelines for the Secure Operation of the Internet" was the result of the Security Policy Working Group. Both of these RFCs are available in the /pub/info directory, as mentioned above.

/pub/tech_tips: The /pub/tech_tips directory contains documents on anonymous FTP configurations, packet filtering, and the CERT security checklist.

/pub/tools: The /pub/tools directory contains various software programs, including COPS, Crack, TCP daemon wrappers, and virus-detection programs.

/pub/virus-l: The /pub/virus-l directory contains the archives and other VIRUS-L and VALERT-L mailing list documents.

B6. What presentations, workshops, and seminars does the CERT Coordination Center offer?

(a) Presentations

Throughout the year, members of the CERT Coordination Center give presentations at various technical conferences, seminars, and regional networks. Periodically, special arrangements can be made to tailor the presentation to fit the requirements of the specific

site. For further information regarding presentations, please contact the CERT Coordination Center. (Contact information is in section A.2.)

(b) Workshops

From 1989 to 1992 the CERT Coordination Center hosted and co-sponsored the FIRST Workshop on Incident Handling. CERT has also participated in subsequent workshops. For further information about the FIRST Workshop on Incident Handling, please contact the CERT Coordination Center.

(c) Seminars

(1) Internet Security for Managers

Description: This seminar is to help managers understand what needs to be done to ensure that their computer systems and networks are as securely managed as possible when operating within the Internet community. Attendees will be provided with information that will enable them to formulate realistic security policies, procedures, and programs specific to their operating environment.

Audience: This seminar is designed for managers of computing centers/facilities, individuals tasked to evaluate/initiate Internet connectivity, senior system administrators, and others interested in computer security within the Internet community.

(2) Internet Security for UNIX System Administrators

Description: The information presented in this seminar is based on incidents reported to the CERT Coordination Center. The topics covered will include defensive and offensive strategies for system administration, site-specific security policies, and incident handling.

Audience: This seminar is designed for users and

system administrators of hosts using the UNIX Operating System. It is especially suited for system administrators of systems connected to a wide area network based on TCP/IP such as the Internet. Some system administrator experience is assumed.

B7. What books or articles does the CERT Coordination Center recommend?

[Bishop 87] Bishop, Matt. "How to Write a Setuid Program." ;login: 12, 1 (Jan/Feb 1987): 5-12.

[Cheswick 94] Cheswick, William R.; Bellovin, Steven M. Firewalls and Internet Security: Repelling the Wily Hacker. New York: Addison-Wesley Publishing Company, 1994.

[Curry 90] Curry, Dave. "Improving the Security of Your UNIX System" (Technical Report ITSTD-721-FR-90-21). Menlo Park, CA: SRI International, April 1990.

[Curry 92] Curry, David A. UNIX System Security: A Guide for Users and System Administrators. Reading, MA: Addison-Wesley Publishing Co., Inc., 1992. (ISBN 0-201-56327-4)

[Denning 91] Denning, Peter J., ed. Computers Under Attack: Intruders, Worms, and Viruses. ACM Press, New York: Addison-Wesley Publishing Company, Inc., 1990. (ISBN 0-201-53067-8)

[Ellis 94] Ellis, Jim; Fraser, Barbara; Pesante, Linda. "Keeping Internet Intruders Away." UNIX Review 12, 9 (September 1994): 35-44.

[Farrow 91] Farrow, Rik. How to Protect Your Data and Prevent Intruders: UNIX System Security.

Reading, MA: Addison-Wesley Publishing Company, Inc., 1991. (ISBN 0-201-57030-0)

[Fithen 94] Fithen, Katherine; Fraser, Barbara. "CERT Incident Response and the Internet." Communications of the ACM 37, 8 (August 1994):108-113.

[Garfinkel and Spafford 91] Garfinkel, Simson; Spafford, Gene. Practical UNIX Security. Sebastopol, CA: O'Reilly & Associates, Inc., 1991. (ISBN 0-937175-72-2)

[Grampo and Morris 84] Grampo, M.; Morris, R.T. "UNIX Operating System Security." AT&T Technical Journal 63, 8 (Oct 1984): 1649-1672.

[Hafner and Markoff 91] Hafner, Katie; Markoff, John. Cyberpunk: Outlaws and Hackers on the Computer Frontier. New York, NY: Simon & Schuster, 1991.

[Morris and Thompson 79] Morris, R.T.; Thompson, K. "Password Security: A Case History." Coomunications of the ACM 22, 11 (November 1979): 594-597.

[Nemeth, Snyder, and Seebass 89] Nemeth, Evi; Snyder, Garth; Seebass, Scott. UNIX System Administration Handbook. Englewood Cliffs, NJ: Prentice Hall, 1989. (ISBN 0-13-933441-6)

[Stoll 89] Stoll, Clifford. The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage. New York, NY: Doubleday, 1989. (ISBN 0-385-24946-2)

[Wood and Kochran 86] Wood, Patrick; Kochran, Stephen. UNIX System Security. Hasbrouck Heights, NJ: Haden Books, 1986.

Section C. Incident Response

C1. What kind of information should I provide to the CERT staff when my site has had an intrusion?

The CERT Coordination Center would like as much information as possible, including opinions and thoughts as to how the break-in occurred. Some specifics include:

1) names of host(s) compromised at your site

2) architecture and OS (operating system and revision) of compromised host(s)

3) whether or not security patches have been applied to the compromised host(s); if so, were patches applied before or after the intrusion

4) account name(s) compromised

5) other host(s)/site(s) involved in the intrusion and whether or not you have already contacted those site(s) about the intrusion

6) if other site(s) have been contacted, the contact information used for contacting the site(s) involved

7) if CERT is to contact the other site(s), can we give the other sites your contact information (i.e., your name, e-mail address, and phone number)

8) whether or not any law enforcement agencies have been contacted

9) appropriate log extracts (including timestamps)

10) what assistance you would like from the CERT Coordination Center