CERT Incident Response and the Internet

Katherine Fithen
Barbara Fraser

The Software Engineering Institute
Pittsburgh Pennsylvania

Abstract: When responding to computer security incidents throughout the Internet community, the CERT Coordination Center utilizes the Internet in many ways. CERT activities involve both individual Internet sites and the global Internet as a whole, and CERT [1] uses resources from the Internet, as well as providing services to the Internet. Included in this paper are discussions of Internet resources employed by CERT, and information on how members of the Internet community can use CERT products and services.

1 Introduction

In 1988, the Advanced Research Projects Agency (ARPA) [2] established the CERT Coordination Center in response to the security risks and issues brought to the attention of the Internet community by the Internet Worm [3]. Since that time, CERT has been an active member of the growing Internet community, and has watched the Internet grow from less than 100,000 hosts to more than 2.2 million hosts [SRI, Inc. 94].

In this relationship, CERT draws upon and uses a number of Internet services and protocols to accomplish its mission, and provides services to the Internet community as well. As the Internet community is the constituency of CERT, it would be difficult to imagine providing CERT products and services without the use of Internet services and protocols.

2 Internet Services Used in Support of Incident Response

One way to understand how valuable Internet resources are to CERT is to look at how those resources are used in support of one of the primary activities of CERT: response to computer security incidents. The following describes a sample incident.

> CERT was contacted by `kathy.org` to report that an intruder has compromised an account with an easily-guessable password on the host `rock.kathy.org`. The site, `kathy.org`, detected the intrusion because users complained of slow response on `rock.kathy.org`. When the system administrator checked to see what processes were running, he noticed that process "Crack" was being run by user "oldman". When the system administrator checked with the account owner of "oldman", it was discovered that an intruder was using the "oldman" account.

Upon further investigation, the file "barbara.pass" was found, and it was a passwd file. The `kathy.org` contact could not identify the owner of the file. CERT agreed to try to identify and contact the site to which the file belonged.

Prior to sending a passwd file across a network, we "sanitize" the file by replacing the encrypted passwords. The CERT incident coordinator assigned to this incident sent a script that replaces encrypted passwords in a password file with "deleted", requested that `kathy.org` run the script on the barbara.pass file, and send the "sanitized" password file to CERT.

After an initial determination of ownership was made, CERT then tried to verify that the passwd file does belong to the particular host by telnetting to the SMTP port (port 25) and using the **vrfy** command. The **vrfy** command verifies that an account name is a valid account on a particular host. This verification is done to ensure that the file is sent to the site to which the file belongs, and not to an incorrect site. This method does not always succeed because some hosts may not allow a telnet connection to the SMTP port, may not allow use of the **vrfy** command, or the **vrfy** command may return whatever was originally entered by the user (e.g., the account name to be verified).

Once the ownership of the password file was determined, CERT then sent the "clean" file to the site, or to the Incident Response Team responsible for the site. Follow-up with site included looking for signs of compromise at that site, and checking to see if other sites were involved. If the site was interested in pursuing a legal investigation, CERT would then provide contact information for the appropriate law enforcement agencies.

Follow-up with the reporting site (`kathy.org`) would include working to determine:

- If the site has any security incident policies and or procedures, and if not, to encourage the development and implementation of such.
- If the site has installed applicable patches or workarounds from CERT advisories, and if not, to do so.
- If the site is using any security tools (e.g., COPS, TCP wrappers, Tripwire, etc.), and if not, to do so.
- To provide documentation on security practices and tools.

Security incidents come in many forms. For example, a valid account could be used by someone other than the account owner, an intruder could gain root access and install a Trojan backdoor, TFTP (Trivial File Transfer Protocol) could be used to obtain a passwd file, or a product vulnerability could be exploited to gain unauthorized access.

Internet services are useful to CERT when receiving and responding to security incident reports. Even when non-computer-based methods, such as the telephone, are used for initial contact with CERT, CERT uses Internet services and protocols for related investigation and follow up. For example, CERT usually receives incident reports in one of two ways:

- A telephone call on the CERT hotline (+1 412-268-7090).
- E-mail to the `cert@cert.org` e-mail address.

A hotline call is often the original report of an incident, but it is then followed-up using e-mail. The exception to this procedure occurs when root access at a site has been compromised, or if a site is disconnected from the Internet; communication may then be conducted by telephone or FAX.

In 1993, CERT handled 1,334 incidents [4]. These 1,334 incidents generated 21,267 pieces of e-mail and 2,282 hotline calls. This represents a 73% increase in the number of incidents in 1993 from 1992, and we expect this type of increase in the number of incidents reported to CERT to continue.

E-mail, FTP, and obtaining site contact information are discussed in further detail in the following sections.

2.1 E-mail

E-mail (electronic mail) is the most prevalent communication mechanism used by CERT. Information received via e-mail allows the Incident Response group to prioritize its work, so that incident mail and informational requests are separated. Responding to incident mail receives a higher priority than responding to informational requests, although CERT currently strives to respond to informational requests within seven days. This also allows the Incident Response group to concentrate on the incident e-mail, therefore providing better service to those sites involved in incidents.

The use of DES-encrypted mail, Privacy Enhanced Mail (PEM) [5], and Pretty Good Privacy (PGP) [6] allows e-mail to be used even when root has been compromised or for discussing product vulnerabilities with vendors via e-mail.

CERT may exchange DES encryption keys with site contacts by telephone, and then e-mail that has been DES-encrypted can be safely exchanged. Note that there are United States export restrictions to which CERT must adhere; DES-encrypted messages can be exchanged, but the DES technology cannot be exported. Other countries have different laws concerning encrypted messages, and CERT must be sensitive to these laws as well.

The concern that e-mail may be read, either by interception or by an intruder reading the clear text copy online is of concern; but of greater concern is that e-mail may be altered while en route. PEM provides a mechanism for e-mail signature certification and for encrypted e-mail. This assures sites that e-mail that appears to have been sent by CERT has indeed be sent by CERT, and that the e-mail has not been altered somewhere en route.

CERT advisories are issued via the cert-advisory mailing list and are also posted to the USENET newsgroup, `comp.security.announce`. The cert-tools mailing list is moderated by CERT, and the purpose of this mailing list is to encourage the exchange of information on tools and techniques that increase the secure operation of Internet systems.

To keep abreast on security issues, members of CERT read USENET newsgroups and mailing lists. Two examples of this type of information are:

- The `comp.security.misc` USENET newsgroup, which is a newsgroup for miscellaneous types of discussions on computer security.
- The mailing list "firewalls", which is an unmoderated mailing list for the discussion of firewall hosts. (To subscribe to the firewalls mailing list, send e-mail to: `Majordomo@GreatCircle.COM` and put "subscribe firewalls" in the body of the message.)

Communication with sites in other time zones is facilitated by the use of e-mail (the e-mail is available when needed and doesn't depend on coordinating time schedules of contacts from different time zones). Also, the language barrier seems to be smaller and less difficult using text e-mail rather than voice.

CERT receives requests to submit articles via e-mail. CERT often e-mails materials to the requester, as was done with this article.

The IETF mailing lists and archived information allow members of CERT to follow and participate in IETF. Much of the IETF information is archived and is available via anonymous FTP.

FIRST, the Forum of Incident Response and Security Teams, communicates via e-mail. CERT is a founding and active member in FIRST. CERT works with FIRST members on incidents and product vulnerabilities. This communication and working relationship assists in resolving incidents and in providing product vulnerability solutions, whether the solutions are patches or "workarounds". CERT also uses DES-encrypted e-mail and PEM with FIRST members when working on incidents and/or product vulnerability reports.

CERT also works closely with FIRST on the Annual FIRST Incident Handling Workshop. Much of this work is done via e-mail; presentation proposals are submitted, topics discussed, etc. This cuts down on travel costs and time, not only for CERT, but all members of FIRST.

E-mail is a very valuable communication tool, but there are several considerations and drawbacks one should be aware of:

- E-mail is easily spoofed.
- E-mail may be intercepted en route or, if left in clear text online, may be seen by an intruder.
- E-mail to root, hostmaster, postmaster, and other generic system administration accounts or aliases may not be read by anyone at the sites.

- E-mail may be sent to aliases, and it may be unclear to whom the alias explodes.
- E-mail loses voice inflection and the immediacy of phone interaction.
- E-mail is not normally automatically acknowledged, therefore CERT may not know if the site received the e-mail sent.
- E-mail sent to the **whois** contact, which may be incorrect (i.e., out-of-date information, incorrect e-mail address), may go unread, may be read by someone else, or may just bounce around the network.
- Services may be interrupted (i.e., a host may be down or there may be network problems).

Spoofing e-mail is learned in first-term computer classes. The novice user may be unaware of this capability, and may be easily fooled by e-mail that appears to have been sent by root or some other system administrator account.

In addition to the concerns of interception and clear text online mail is the concern of mail sent to the wrong e-mail address. Since there is no automatic acknowledgment that e-mail has been received, CERT may not receive any response from e-mail sent to a site; therefore there is no way to be certain that the e-mail has been received by the correct addressee.

The loss of voice inflection when using e-mail has improved with the use of "standard" notations, such as the sideways smiley face " :-) ". Use of these notations is important to denote humor, sadness, sarcasm, etc. Without these notations, the reader interprets the e-mail from only their own frame of reference. This can lead to misunderstandings, bad feelings, and/or "flames".

2.2 Anonymous FTP

Anonymous FTP (File Transfer Protocol) is used by CERT to receive incident-related files from sites, to provide and to gather information to and from the Internet community. Many sites use anonymous FTP on `info.cert.org` to send files to CERT for review. CERT has created an incoming directory that is writable, but not readable, on this host. Configuring the incoming directory in this way allows sites to use anonymous FTP to transfer files to CERT, but users can use neither the **ls** nor the **dir** command to list the contents of the directory. The deposit of a file is logged and automatic notification to CERT team members is sent via e-mail.

CERT archives much security-related information, and it is available via anonymous FTP from `info.cert.org` in the `/pub` directory. Some of the information archived includes:

- An archive of CERT advisories.
- An archive of virus information.
- An archive of security tools.
- An archive of security papers and technical documents.
- IETF security-related RFCs (Request for Comments).
- A clipping service (a central archive repository for selected security related USENET News and mailing list postings).

Archived information available via anonymous FTP, whether it is archived by CERT or by another site, is very valuable. For example, some vendor security patches are available via anonymous FTP from `ftp.uu.net`; if that host is unreachable, then a user can use archie to obtain a list of other hosts that provide that information via anonymous FTP.

Much of the research done at CERT is based on information provided by the Internet community via either e-mail or anonymous FTP. Research collaboration is also a benefit to CERT and its constituents.

Again, as with e-mail, there are considerations and drawbacks to be considered when using FTP:

- Abuse of anonymous FTP areas can occur.
- Services may be interrupted (i.e., a host may be down or there may be network problems).

The abuse of anonymous FTP areas is a concern of the Internet community. Making information freely and easily available is a fundamental belief of the Internet community. Creating anonymous FTP areas for Internet users to share information is considered to be a "good" thing. Unfortunately, some users have used anonymous FTP areas for exchanging pirated commercial software, and for sharing intruder information (e.g., scripts to exploit vulnerabilities, compromised account information, etc.). And, archie information has been exploited to identify sites which provide writable anonymous FTP areas. An intruder could use a listing from an archie search to create hidden directories in those writable anonymous FTP areas to be used for pirating software.

To prevent the abuse of anonymous FTP areas, CERT has created a document on the suggested configuration of an anonymous FTP area. This document is available via anonymous FTP from `info.cert.org` and the path for the file is:
`/pub/tech_tips/anonymous_ftp`.

2.3 Contact Information

When sending security incident information to a site, CERT generally uses various **whois** databases to find domain contacts for sites. (Note that some sites have designated specific contacts at their sites for security incidents.) Information from the **whois** databases is available via telnet and anonymous FTP:

- `rs.internic.net` for all domain contacts from the InterNIC **whois** database.
- The WAIS server `info.ripe.net` (192.87.45.1) for European sites.
- `nic.ad.jp` (192.41.192.41) for Japanese sites (the `.jp` domain). You may want to specify that you would like the result of the search in English, as the default is Japanese.
- Files available via anonymous FTP from `relay.cdnnet.ca` (192.73.5.1) for Canadian sites (the `.ca` domain).

The InterNIC **whois** information for non-US domains provides the contact information for the entire regional domain (e.g., the contact for "jp-dom" is the contact for the Japan top-level domain [`.jp` domain]).

If a site needs contact information, CERT can provide assistance in accessing these.

3 CERT Future Directions and Plans

With the tremendous growth of the Internet, CERT realizes that making information available in a variety of ways is important to the success of CERT. CERT is investigating the possibility of providing information via network information resource services such as Wide-Area Information Server (WAIS) and World-Wide Web (WWW).

Also important to the success of CERT is the automation of requests for information. CERT receives about 40 informational requests per week. While this may not sound like a large number of requests, in the midst of approximately 500 e-mail message per week, it is significant. CERT is considering using an automatic mail server, such as LISTSERV, and/or FTP mail, to automate information and mailing list requests and as a second distribution mechanism for lower-level information.

Currently, the principal method for dissemination of security-related information from CERT to the Internet community is a CERT advisory. Associated with an advisory is an expected level of urgency for the information in the advisory. CERT recognizes that there are different levels of urgency for security-related information. An example of a way to address these different levels of urgency may be to have several levels of information. A CERT "alert" may contain information of the highest level of urgency, while a CERT "warning" may contain important information, but not as urgent as an alert, while a CERT advisory may contain advisory information or suggestions, which hold little urgency, but yet are still important information to provide to the Internet community. An example of this “advisory” level information is the CA-92:19.Keystroke.Logging.Banner.Notice advisory. This advisory was a suggestion for a host login screen from the Department of Justice “as a method of protecting computer systems from unauthorized access.”

4 CERT Future Technology Needs

A few of the short-term technology needs of CERT include:

- Wide-spread Internet use of PEM, or similar technologies.
- Wide-spread Internet use of one-time passwords.
- IP encryption.

CERT participated in a beta-testing of Trusted Information Systems, Inc. (TIS) PEM, and information has been exchanged with other beta-test sites. CERT sees the need for PEM to be widely distributed to the Internet community to ensure trust that the information that appears to have come from CERT does indeed come from CERT, and that the information has not been altered in any way.

CERT has found one-time password authentication to be a more secure way to connect to hosts via an Internet connection. Even if this one-time password is intercepted, it is un-usable by an intruder since the one-time password is changed each time a login occurs. CERT would like to see this type of technology widely used by the Internet community. Currently, there are both public and proprietary products available.

IETF has a working group, the IPSEC working group, investigating and developing IP encryption technologies. The IP encryption technologies being investigated would encrypt the data/contents of the IP packet, but not the header information, and then encapsulate the IP packet to send across the Internet. This will protect the data so that if others “see” the packet as it travels across the Internet, the data is unreadable without the encryption key. CERT supports the development of this capability.

5 Closing

The CERT constituency is the Internet community, and it is natural that CERT uses the Internet to both obtain and provide information and services. In spite of the challenges of working in this huge internet-worked environment, CERT could not provide reasonable service to such a vast constituency without the use of the Internet services and protocols. CERT will continue to encourage the integration of security in the development of the Internet. The relationship between CERT and the Internet continues to be beneficial to both.

6 Author Information

Katherine Fithen is a Technical Coordinator in the Incident Response group of the CERT Coordination Center. The CERT Coordination Center provides assistance to Internet sites that have computer security issues, concerns, or have experienced a computer security compromise. Prior to joining CERT, she was a User Consultant for PREPnet, the regional network service provider for the state of Pennsylvania. Katherine has earned a Bachelor's degree in Retail Management, a Master's degree in Personnel Management, and a Master's degree in Information Science.

Barbara Fraser is the manager of the Security Improvement Group for the CERT, the Computer Emergency Response Team located at Carnegie Mellon University, in the Software Engineering Institute (SEI). Her responsibilities include the planning and development of security-related products. Barbara has given many talks and classes on CERT and Internet security, and she has worked with many organizations to help them understand security issues as they relate to the Internet. Barbara is active in the security area of the Internet Engineering Task Force and was one of the authors of RFC 1281, “Guidelines for the Secure Operation of the Internet”.

Barbara holds a Bachelor’s degree in Biology, and a Master’s degree in Computer Science.

7 Endnotes

[1] Informally, the CERT Coordination Center is referred to as "CERT" throughout this and other documents. For further background information on the establishment of the CERT Coordination Center, see [Fraser 92].

[2] ARPA was formerly DARPA (the Defense Advanced Research Projects Agency).

[3] For more information on the Internet Worm, there are several books and articles. One suggestion may be [Curry 92].

[4] Note that an incident may involve one site or hundreds (or even thousands) of sites. Also, some incidents may have ongoing activity for long periods of time - up to more than a year.

[5] For further information on PEM, see RFCs 1113, 1114, and 1319, available via anonymous FTP. There have been several papers published on the topic of PEM; see [Bishop 93] and [Kent 93].

[6] For further information on PGP, contact Viacrypt, Inc.

8 Bibliography

[Bishop 91] Bishop, M. "Privacy-Enhanced Electronic Mail," *Journal of Internetworking: Research and Experience* 2(4). December 1991.

[Bishop 93] Bishop, M. "Recent Changes to Privacy-Enhanced Electronic Mail," *Journal of Internetworking: Research and Experience* 4(1). March 1993.

[Comer 91] Comer, D., *Internetworking with TCP/IP Vol I: Principles, Protocols, and Architecture*. Second ed. Prentice-Hall, Inc. 1991.

[Curry 90] Curry, Dave. Improving the Security of Your UNIX System (Technical Report IT-STD-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.* Addison-Wesley Publishing Co., Inc. (ISBN 0-201-56327-4), 1992.

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

[Fraser 92] Fraser, Barbara F., & Pethia, Richard D. The CERT/CC Experience: Past, Present, and Future. *Proceedings of INET'92. Internet Society*, 1992.

[Galvin 92] Galvin, James M. and David M. Balenson. *Security Aspects of a UNIX PEM Implementation*. USENIX Security Symposium III, September 14-16, 1992.

[GAO 89] United States General Accounting Office. *Computer Security: Virus Highlights Need form Improved Internet Management*. United States General Accounting Office (GAO/IMTEC-89-57), 1989.

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

[Holbrook 91] Holbrook, J. Paul, & Reynolds, Joyce, Editors, *Site Security Handbook*, FYI 8, RFC 1244, CicNet, ISI, July 1991.

[Kent 93] Kent, Stephen T. "Internet Privacy Enhanced Mail." *CACM* 36 (August 1993): 48-61.

[Morris 79] Morris, R.T.; Thompson, K. *Password Security: A Case History*. CACM 22 (November 1979): 594-597.

[Pethia 91] Pethia, Richard D., Crocker, Stephen D., & Fraser, Barbara Y., *Guidelines for the Secure Operation of the Internet*, RFC 1281, SEI, TIS, November 1991.

[Scherlis 90] Scherlis, William, L., Squires, Stephen L., & Pethia, Richard D., Computer Emergency Response, in Denning, P., editor, *Computers Under Attack: Intruders, Worms, and Viruses*, ACM Press, Reading, Massachusetts, 1990, pp. 495-504.

[SRI International 94] SRI International Network Information Systems Center. *Internet Domain Survey*, January 1994.

[Tardo 91] Tardo, Joseph, J. & Alagappan, Kannan, SPX: Global *Authentication Using Public Key Certificates, Proceedings of the 1991 IEEE Computer Society Symposium on Research in Security and Privacy*, Oakland, California, May 1991, pp. 232-244.

CERT is sponsored by the Advanced Research Projects Agency (ARPA).

The Software Engineering Institute is sponsored by the U.S. Department of Defense.