Administrators Guild), and ISSA (Information Systems Security Association, Inc.).

Prior to joining CERT, Katherine was a User Consultant for PREPnet, the regional network service provider for the state of Pennsylvania.

Katherine has earned a bachelor's degree and a master's degree from Louisiana Tech University, and a master's degree in Information Science from the University of Pittsburgh.

Katherine may be reached at: kfithen@cert.org.

Barbara Fraser is the manager of the product development 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 tutorials and other security-related products. Barbara is responsible for conducting tutorials, seminars, and workshops, and she also coordinates CERT's vendor program. 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". She is also an active member of the Security Area Advisory Group within the IETF.

Prior to joining the SEI, Barbara worked for the Electronic and Missiles Systems Division of Martin Marietta Corporation in Orlando, Florida where she was task leader for a software development group. Barbara's background also includes teaching Computer Science courses at the university level.

Barbara holds a bachelor's degree from Florida State University and a master's degree in computer science from the University of Central Florida.

Barbara may be reached at: byf@cert.org.

JPO #93-135
ESC #93-0553

authentication to be a more secure way to connect to hosts via an Internet connection. Even if this key is intercepted, it is un-usable by an intruder since the key 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. CERT supports the development of this capability.

VIII. 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 several considerations and drawbacks previously mentioned, 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.

X. Bibliography

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

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

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

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

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

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

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

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

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

[10] Rutkowski, A. M. Internet Metrics. Internet Society News, Vol. 2, No. 1, Spring 1993: 34-38.

[11] Morris, R.T.; Thompson, K. "Password Security: A Case History." CACM 22(11) (November 1979): 594-597.

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

[13] 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.

[14] 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.

Author Information

Katherine Fithen is a Technical Coordinator in the Incident Response group for CERT. Her responsibilities include providing technical assistance and support to sites on the Internet that have experienced a computer security incident. Katherine is a member of SAGE (Systems

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 sure 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. If not used, the sender may receive an unexpected response, such as a "flame," a response of dissatisfaction for the message received.

The abuse of the anonymous FTP area is a more serious drawback of the Internet. 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, the intruder community has used anonymous FTP areas for exchanging pirated commercial software. And, archie information has been exploited to list sites which provide anonymous FTP areas. An intruder could use a listing from an archie search to create hidden directories in those anonymous FTP areas to be used for pirating software.

"Hidden" directories are those not found by the simple "ls" command, such as ".. " (dot dot space space), in areas that are writable and readable. A site may check for inappropriate use, but might not do an "ls -laR" rather than an "ls" to check for directories. In this case, the hidden directories would not be listed, and therefore would still be usable. A site should use "find" or "ls -laR" to search for hidden directories.

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 cert.org and the path for the file is:
/pub/tech_tips/anonymous_ftp.

VI. 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 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 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 information important, 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."

VII. CERT Future Technology Needs

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

- Wide-spread Internet use of PEM.
- Wide-spread Internet use of one-time passwords.
- IP encryption.

CERT is beta-testing 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

e-mail rather than voice.

While traveling, CERT team members can connect to CERT hosts either by dialing in or by using an Internet connection, if available. Given a choice between a dial-up connection and an Internet connection, an Internet connection provides better connectivity and response than a dial-up connection. However, to ensure that captured passwords can't be used in the future to compromise CERT hosts, CERT team members use a one-time challenge/response password technology to connect to a host via an Internet connection.

CERT receives requests to present at conferences, workshops, etc. via e-mail. CERT often e-mails presentation materials to the presentation requester, as was done with this presentation.

Providing contact information and the knowledge of how to obtain that information helps CERT by putting sites in direct communication with each other, rather than CERT acting as a "middle man.

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 (192.48.96.9); if a host is unreachable, then a list of hosts that provide that information via anonymous FTP from archie indicates other hosts from which the information can be obtained. Using archie to find information available via anonymous FTP can save time when looking for information.

The IETF mailing lists and archived information allow members of CERT to follow and participate in IETF without having to send all participating staff to the IETF meetings

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" to the OS (operating system). CERT also uses DES-encrypted e-mail and PEM with FIRST members when working on incidents and/or product vulnerability reports. The use of e-mail allows members of CERT to follow and participate in FIRST without having to attend the FIRST meetings.

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.

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.

V. Considerations/Drawbacks of Internet Services and Protocols

There are several considerations and drawbacks to be aware of in using the Internet services and protocols:

- 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 sent to the whois contact, which may be incorrect (i.e. out-of-date information, incorrect e-mail address), may be read by someone else, or may just bounce around the network for a while.
- E-mail to root, hostmaster, postmaster, and other generic system administration accounts may not be read by anyone at the sites.
- E-mail is not automatically acknowledged, therefore CERT may not know if the site received the e-mail sent.
- E-mail loses voice inflection and the immediacy of phone interaction.
- Abuse of anonymous FTP areas can occur.
- 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, and used. 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.

The concern that e-mail may be read, either by interception or by an intruder reading the clear text copy online is of greater concern. CERT addresses this problem by using DES encryption and PEM.

In addition to the concerns of interception and clear text online mail is the concern of mail sent to

- nic.ad.jp (192.41.192.41) for Japanese sites (the .jp domain). Although, 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]).

In addition to providing security documentation available from CERT, there are other resources that CERT assists sites in finding and using. One example of this type of activity is finding information (in the form of documents, patches, or source code) available via anonymous FTP. Archie, a program that provides a list of hosts that make information available via anonymous FTP, may be used. This allows the user to locate host(s) which offer the information sought. Having a listing of several sites that archive the information is helpful in case a particular host is unreachable. Sites ask CERT where to find resources; CERT may use archie to answer these requests. CERT also informs sites on the use of archie, so that sites can find information for themselves.

To stayed informed on security issues, members of CERT read USENET newsgroups, such as comp.security.misc, which is a newsgroup for miscellaneous types of discussions on computer security, and mailing lists, such as the firewalls mailing list, 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.)

Members of the CERT team actively participate in the Internet Engineering Task Force (IETF), often via the e-mail mailing lists. Much of the IETF information is archived and is available via anonymous FTP.

III. CERT Products and Services and the Internet

As noted previously, CERT uses Internet services and protocols, including E-mail, FTP, and USENET newsgroups to provide its products and services.

One of the CERT products is 24-hour availability to assist Internet sites for emergency incident response. Regular business hours for the CERT Coordination Center are 8:30am-5:00pm, EST/EDT, Monday-Friday.

Again, most of CERT interaction with constituents is via e-mail, whether this involves an intrusion or reporting a product vulnerability to a vendor. If a site needs contact information, CERT instructs that site on the use of the various whois databases.

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.

CERT archives much documentation; this documentation is available via anonymous FTP from cert.org in the /pub directory. This information includes an archive of CERT advisories, IETF security-related RFCs (Request for Comments), an archive of virus information, an archive of tools available to assist sites in securing their hosts, a clipping service which is a central archive repository for selected security related USENET News and mailing list postings, and security-related documentation.

IV. Benefits of Internet Services and Protocols

CERT derives many benefits from the use of the Internet. Information received via e-mail allows the Incident Response group to prioritize its work, such 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 three 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.

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

been compromised, or if a site is disconnected from the Internet; communication may then be conducted by telephone or FAX.

The use of DES-encrypted mail and Privacy Enhanced Mail (PEM)[1] allows e-mail to be used even when root has been compromised. CERT may also 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; CERT must be sensitive to these laws as well.

PEM 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 en route.

Many sites use anonymous FTP on cert.org (192.88.209.5) to send compressed and DES'd 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 FTP 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 hostmaster for cert.org takes place via e-mail.

After the file(s) are in this directory, the reporting site calls or sends e-mail to tell CERT the name(s) of the file(s). CERT then moves the files to a host behind the firewall host; this host behind the firewall is inaccessible from outside the organization. CERT uses the information from these files to:

- Look for host(s)/site(s) involved in the incident.
- Look for how the host(s)/site(s) are involved in the incident.
- Track MOs (modus operandi).
- Conduct CERT research.

Examples of ways host(s)/site(s) can be involved in an incident include the following:

- Host(s) at a site are compromised.
- Legitimate account(s) on host(s) are used for unintended purposes.
- An intruder gains unauthorized access to services offered by the host(s)/site(s).
- A passwd file for a host is found on another host.

One example of the files received by CERT is a passwd file from one site found at a different site involved in an incident. This may indicate an intrusion at either or both sites. In such circumstances the first concern to CERT is to determine the ownership of the passwd file. After that initial determination is made, CERT may verify that the passwd file does belong to the particular host by telnetting to port 25 (the SMTP port) and using the "vrfy" command. 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. The "vrfy" command verifies that an account name is a valid account on that host.

Note that some hosts may not allow a telnet connection to the SMTP port, or may not allow use of the "vrfy" command.

Prior to sending the passwd file to the site to which CERT believes the file belongs, CERT "cleans" the file with a script that removes the encrypted passwords. This prevents sending passwords, although encrypted, in clear text across the network. This script has also been made available to sites so that the sites can remove the encrypted passwords from the files prior to sending the files to CERT.

When sending security incident information to a site, CERT generally uses the 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. The InterNIC whois information is available from rs.internic.net (198.41.0.5), and the DDN NIC whois information is available from nic.ddn.mil (192.112.36.5). Only DDN (.mil domain) whois information is available from the DDN NIC whois database; non-.mil domain whois information is available from the InterNIC.

Other region-specific whois information is available from:

- The WAIS server info.ripe.net (192.87.45.1) for European sites.

1. For further information on PEM, see RFCs 1113, 1114, and 1319, available via anonymous FTP.

CERT Incident Response and the Internet

Katherine T. Fithen[1]
Barbara Y. Fraser[2]

Abstract

When responding to computer security incdents 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[3] 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.

I. Introduction

In 1988, the Advanced Research Projects Agency (ARPA)[4] 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. 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 1.3 million hosts [10].

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.

II. Uses of Internet Services 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: security incident response. 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 could be used to obtain a passwd file; or a product vulnerability could be exploited to gain unauthorized access.

These services are useful to CERT in many ways, including 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.

In 1992, CERT handled 773 incidents[5]. These 773 incidents generated 14,463 pieces of e-mail and 1,995 hotline calls. The hotline calls are often the original report of an incident, which are then followed-up via e-mail. The exception to this procedure occurs when root access at a site has

1. Katherine T. Fithen
Technical Coordinator
CERT Coordination Center
kfithen@cert.org

2. Barbara Y. Fraser
Technical Coordinator
CERT Coordination Center
byf@cert.org

3. 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 [5].

4. ARPA was formerly DARPA (the Defense Advanced Research Projects Agency).

5. 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.