-- --

Computer Emergency Response - An International Problem†

Richard D. Pethia
Kenneth R. van Wyk

Computer Emergency Response Team / Coordination Center
Software Engineering Institute
Carnegie Mellon University
4500 Fifth Avenue
Pittsburgh, PA 15213-3890
U.S.A.

ABSTRACT

Computer security incidents during the past few years have illustrated that unauthorized computer activity does not obey traditional boundaries (e.g., national, network, computer architecture). Instead, such activity frequently crosses these boundaries not just once, but several times per incident [Stoll89].

International cooperation among computer security response groups can be an effective means of dealing with computer security issues faced today by the computer user community. This paper addresses the need for such cooperation and suggests methods by which individual computer security response groups can work together internationally to cope with computer security incidents.

1. Background

The increasing use and dependence on interconnected local, regional, and wide area networks, while bringing important new capabilities, also brings new vulnerabilities. Widely publicized events such as the November 1988, Internet Worm, which affected thousands of systems on the international research network Internet, or the October 1989, WANK worm, which affected hundreds of systems on NASA's Space Physics and Analysis (SPAN) network are unusual, although dramatic, events. There are many more events such as intrusions, exploitation of vulnerabilities, and discovery of new vulnerabilities that occur with much greater frequency and require effective methods of response. Several examples are listed below.

1.1. Incidents

From August 1986 until late 1987, staff members at Lawrence Berkeley Laboratory worked with investigators to trace the paths of a computer intruder; the trail eventually lead them to a KGB-funded intruder operating out of Hannover, Germany [Stoll88]. The investigation was often hampered by a lack of cooperation among "bureaucratic organizations" [Stoll88]. On the other hand, "cooperation between system managers, communications technicians, and network operators was excellent" [Stoll88]. Still, it was only when the investigators in both countries got involved that the intruder was apprehended [Stoll89]. It is worthwhile to note that the break-ins in this case utilized the same attack methods over and over (such as repeatedly guessing common and system default username/password combinations, exploiting well known security holes which had not yet been fixed by the system administrators, etc.); through diligent, methodical application of these methods, the intruders were successful at entering dozens of

‡ Sponsored by the U.S. Department of Defense

-- --

computer systems [Stoll89].

In November 1988, a rogue worm program entered the Internet and caused widespread system failures [Spafford88]. The worm, written by Cornell University graduate student Robert Tappan Morris, Jr. [Markoff90a], exploited lax password policies as well as two software implementation errors in specific versions of UNIX, the predominant operating system on Internet computers.

More recently, three Australian computer intruders were arrested by Australian Federal police "after a two-year investigation that included cooperation with United States authorities" [Markoff90b]. Again, the intruders exploited known vulnerabilities to gain unauthorized entry onto systems [Danca90].

In October 1989, a worm program called Worms Against Nuclear Killers (WANK) infected a National Aeronautics and Space Administration (NASA) network [Alexander89]. The worm program spread to many computers in different countries by using system vulnerabilities that "should have been closed months ago" following a similar incident in December 1988 [Alexander89].

In another, albeit domestic, case, two computer intruders were arrested and charged with illegal use of computer systems at Pennsylvania State University. The intrusions took place on a computer system at the University of Chicago. University of Chicago officials contacted CERT/CC, which then contacted administrators at Penn State. Eventually, through the cooperation of the administrators and investigators, the two Penn State students were charged [Graf90].

These cases all illustrate the need for cooperation among computer security response groups.

1.2. System Vulnerabilities

Another situation in which cooperation across multiple organizations becomes essential is in dissemination of system vulnerability alerts (and, more importantly, their solutions). As system intruders successfully gain access to systems which have weak passwords or systems where known security vulnerabilities have not been closed, they often share information on vulnerabilities in these systems with others. Likewise, as intruders discover new vulnerabilities in particular operating system or other software packages, information on the vulnerabilities is quickly communicated through various bulletin boards and other electronic forums.

As a result, many large communities of system users quickly become vulnerable. Traditional methods of dealing with vulnerability information, including closely protecting information on the existence of the vulnerability, are not effective once intruders have learned of system weaknesses. In these cases, supplying password guideline and security vulnerability information to system administrators is crucial in raising security levels and deterring attacks.

The Computer Emergency Response Team Coordination Center (CERT/CC) (see Section 2.1) frequently distributes CERT Advisories that, among other things, inform the public of vulnerabilities, fixes, and active methods of attack.

2. Emergency Response Groups

2.1. Introduction to CERT

Shortly after the Internet worm of November 1988 [Spafford88], the Defense Advanced Research Projects Agency (DARPA) started the Computer Emergency Response Team (CERT), whose Coordination Center (CERT/CC) is located at Carnegie Mellon University's Software Engineering Institute (SEI) [Scherlis88]. "The CERT is a community group intended to facilitate community response to computer security events involving Internet hosts" [Denning90]. CERT consists of hundreds of highly qualified volunteers throughout the computer community, as well as the staff of the CERT/CC and of the other emergency response groups in the CERT-System (see Section 2.2 for details). The CERT/CC serves as a focal point for response to Internet computer security problems [Denning90]. Since it would be impossible for any one response group to address the needs of all constituencies‡, the need for multiple CERT

‡ The term "constituency" is used here to define a group with some common needs.

groups exists. (This issue, too, is covered in more detail in Section 2.2.)

CERT groups must have sufficient in-house technical expertise to handle a reasonable portion of day to day security incidents, leaving the volunteer contacts for situations which require additional expertise. However, because emergency response involves addressing more than just technical issues, CERT membership includes not only technical experts, but site managers, security officers, industry representatives, and government officials [Denning90].

One of the essential characteristics of a CERT group is being available to its constituency on a 24 hour per day basis. There must be a well publicized central point of contact which is available continuously. This should include, at a minimum, a "hotline" telephone which is constantly manned, and an electronic mailbox which is monitored during business hours. The CERT/CC hotline number is (412) 268-7090, and its electronic mailbox address is cert@cert.sei.cmu.edu, on the Internet.

It is critical that a CERT group build and maintain a collection of contacts, both within the group's constituency and externally [Dalton90]. The contact information should include other CERT groups, system vendors, law enforcement, network operation centers, technical experts, site administrators, etc. Building the contact information is an on-going process in which contacts are developed and maintained over time. Each contact must be aware of its responsibilities and/or expectations in the emergency response process [Dalton90].

In addition to the contact information, a CERT group should maintain an information repository which will be drawn upon in future incidents. The information in the repository will include contact information (as detailed above), system vulnerability details, security incident reports, electronic mail archives, and other relevant information [Denning90]. Due to the nature of this information, the security on the system on which it resides must be beyond reproach. CERT/CC maintains its information database on an off-line system, which is not accessible via network connections.

As system vulnerabilities (and their fixes), break-in warning information, and other relevant information becomes available, CERT groups should issue advisories to members of their constituency [Denning90]. Past CERT/CC advisories have included vulnerability notification (along with appropriate solutions), warnings of widespread break-ins and symptoms thereof, and secure system administration suggestions. The entire collection of CERT/CC advisories are maintained on-line and are accessible to CERT/CC constituents.

2.1.1. Example CERT Incident Handling Procedures

As an ongoing process, CERT/CC has developed and is continuing to improve upon its event handling procedures. Naturally, the procedures are different for each distinct type of event (e.g., system break-in, vulnerability report, worm). This section presents an overview of some of these procedures.

When CERT/CC receives a report of a system break-in, it first works together with the affected system administrator(s) in determining how the intruder gained access to the system. This is generally in the form of offering guidance on what sort of signs the administrator should look for to determine means of access. Next, CERT/CC offers assistance in repairing the exploited hole(s), as well as other commonly known vulnerabilities. Examining systems for backdoors or trojan horses that have been planted by the intruder is an especially important activity. If the break-in came from other sites, or if the intruder broke into other systems from the current system, CERT/CC notifies other affected site administrators (from time to time, the administrator will already have contacted other affected sites; in such a case, CERT/CC requests to be kept up to date with the relevant flow of information between the sites). In some cases, other affected, or potentially affected, sites are not Internet sites. In these cases, communication across traditional "territorial" boundaries is especially important. It is important to note that, when contacting sites, CERT/CC always maintains the confidentiality of the affected sites unless the sites specify otherwise.

As system vulnerabilities are reported to CERT/CC, they are first authenticated and then reported to the affected vendor(s). CERT/CC offers guidance to the vendor community by reporting the magnitude of the threat (e.g., whether the hole is being actively exploited, whether the hole is known to a widespread audience, whether the hole can be exploited from a remote system or requires existing system access in order to be exploited). CERT/CC also offers technical input, if desired by the vendors. The vendor community will generally respond with a fix, a workaround, or a reference to same for the problem. In many cases, the CERT/CC has received advanced versions of fixes from vendors and has received the vendor's authorization to release the fix to selected members of the technical community for review and comment. This technical review process shows promise of improving the quality of corrections to vulnerabilities.

Depending upon the situation, CERT/CC then drafts an advisory for review by the vendors, the CERT-System, and/or technical affiliates. When the draft advisory is mutually accepted, it is distributed electronically to CERT/CC's constituency, the Internet research community. For this, CERT/CC operates a CERT Advisory mailing list, in addition to a Usenet newsgroup, comp.security.announce [Quarterman90]. (See Appendix 1 for an example CERT/CC advisory.)

2.2. CERT-System

As mentioned in Section 2.1, no single emergency response group can be expected to address the needs of every portion of the computing world, due to the diversities and scale of all of the various computing environments [Denning90]. Individual communities each have their own distinct policies, rules, regulations, procedures, and culture. Methods effective in one community (e.g., the Internet research community) would not likely succeed in other communities that have significantly different cultures (e.g., the military community or the banking community).

In addition, implementation platforms (operating systems, networking software and protocols) vary widely. A single CERT group would not likely be successful in dealing with technical diversity, or at least could not do so economically.

The "CERT-System" model, therefore, includes multiple, cooperating individual CERT organizations. Each individual CERT group in the CERT-System focuses on a particular constituency.

Each constituency in the model can be defined by either user or technology boundaries. The user constituencies consist of groups with common networks, needs, and/or policies, while the technology constituencies are groups with common computing architectures [Denning90]. An example of a user constituency is the Internet research community, which is made up of organizations in academia, government, military, as well as commercial groups. These groups are bound together by being members of the Internet network. An example technology constituency is the IBM mainframe community, which is bound by a common computer architecture.

The CERT/CC group addresses both a user constituency (Internet research community) and a technology constituency (UNIX-based workstations and mainframes, which is the primary type of system on the Internet).

The CERT model lends itself well to network groups such as the Internet research community, as well as corporate [Fedeli90], government, military, etc., groups.

In times of crisis, many CERT groups can be active with a technology coordination center analyzing problems and coordinating the search for solutions and with user constituency coordination centers gathering information and informing their constituents as appropriate.

In less troubled times, the CERTs work together to build effective communication mechanisms, share information on effective computer security tools and techniques, and conduct proactive campaigns aimed at increasing the awareness of computer security issues and improving the security of operational systems.

The CERT-System model has been widely accepted and eleven groups funded by U.S. government agencies and several private firms now participate in the system. Interest in participating has been expressed by several other organizations and steps are being taken to more formally structure the CERT-System. This structure, including a charter and by-laws that are being reviewed and approved by existing CERT-System members as this paper is being written, will provide a framework to enable wider participation.

3. Conclusions

It has been shown that the CERT concept can be an effective means of responding to computer security-related incidents [Graf90]. In incidents prior to the existence of CERT, system administrators were frequently at a loss for outside assistance when handling security incidents [Stoll88, Stoll89]. It has also been shown that computer system security incidents do not obey network, national, or architectural boundaries [Stoll88] and that the intruders frequently exploit lax security procedures (due, perhaps, to a lack of specific knowledge on the administrators' part) [Stoll88, Danca90, Alexander89].

Effective computer security incident response requires communication and coordination across multiple communities. While many incidents occur because software design or implementation deficiencies are exploited, resolution of the incidents requires more than a technical solution. Communication of threat and vulnerability information across computing communities is essential to resolving specific incidents and improving the security of operational systems.

A well formed CERT-System will raise security awareness and knowledge among site administrators as well as give the administrators sources of assistance in times of computer emergencies. By drawing on the experiences of individual CERT groups, the knowledge level of the CERT-System as a whole will grow, enabling all members to more effectively and efficiently deal with computer security incidents as they arise.

1. Example CERT/CC Advisory

CA-90:02

CERT Advisory
March 19, 1990
Internet Intruder Warning

There have been a number of media reports stemming from a March 19 New York Times article entitled 'Computer System Intruder Plucks Passwords and Avoids Detection.' The article referred to a program that attempts to get into computers around the Internet.

At this point, the Computer Emergency Response Team Coordination Center (CERT/CC) does not have hard evidence that there is such a program. What we have seen are several persistent attempts on systems using known security vulnerabilities. All of these vulnerabilities have been previously reported. Some national news agencies have referred to a 'virus' on the Internet; the information we have now indicates that this is NOT true. What we have seen and can confirm is an intruder making persistent attempts to get into Internet systems.

It is possible that a program may be discovered. However, all the techniques used in these attempts have also been used, in the past, by intruders probing systems manually.

As of the morning of March 19, we know of several systems that have been broken into and several dozen more attempts made on Thursday and Friday, March 15 and 16.

Systems administrators should be aware that many systems around the Internet may have these vulnerabilities, and intruders know how to exploit them. To avoid security breaches in the future, we recommend that all system administrators check for the kinds of problems noted in this message.

The rest of this advisory describes problems with system configurations that we have seen intruders using. In particular, the intruders attempted to exploit problems in Berkeley BSD derived UNIX systems and have attacked DEC VMS systems. In the advisory below, points 1 through 12 deal with Unix, points 13 and 14 deal with the VMS attacks.

If you have questions about a particular problem, please get in touch with your vendor.

The CERT makes copies of past advisories available via anonymous FTP (see the end of this message). Administrators may wish to review these as well.

We've had reports of intruders attempting to exploit the following areas:

1) Use TFTP (Trivial File Transfer Protocol) to steal password files.

To test your system for this vulnerability, connect to your system using TFTP and try 'get /etc/motd'. If you can do this, anyone else can get your password file as well. To avoid this problem, disable tftpd.

In conjunction with this, encourage your users to choose passwords that are difficult to guess (e.g. words that are not contained in any dictionary of words of any language; no proper nouns, including names of "famous" real or imaginary characters; no acronyms that are common to computer professionals; no simple variations of first or last names, etc.) Furthermore, inform your users not to leave any clear text username/password information in files on any system.

If an intruder can get a password file, he/she will usually take it to another machine and run password guessing programs on it. These programs involve large dictionary searches and run quickly even on slow machines. The experience of many sites is that most systems that do not put any controls on the types of passwords used probably have at least one password that can be guessed.

2) Exploit accounts without passwords or known passwords (accounts with vendor supplied default passwords are favorites). Also uses finger to get account names and then tries simple passwords.

Scan your password file for extra UID 0 accounts, accounts with no password, or new entries in the password file. Always change vendor supplied default passwords when you install new system software.

3) Exploit holes in sendmail.

Make sure you are running the latest sendmail from your vendor. BSD 5.61 fixes all known holes that the intruder is using.

4) Exploit bugs in old versions of FTP; exploit mis-configured
anonymous FTP

Make sure you are running the most recent version of FTP which is the Berkeley version 4.163 of Nov. 8 1988. Check with your vendor for information on configuration upgrades. Also check your anonymous FTP configuration. It is important to follow the instructions provided with the operating system to properly configure the files available through anonymous ftp (e.g., file permissions, ownership, group, etc.). Note especially that you should not use your system's standard password file as the password file for FTP.

5) Exploit the fingerd hole used by the Morris Internet worm.

Make sure you're running a recent version of finger. Numerous Berkeley BSD derived versions of UNIX were vulnerable.

Some other things to check for:

6) Check user's .rhosts files and the /etc/hosts.equiv files for systems outside your domain. Make sure all hosts in these files are authorized and that the files are not world-writable.

7) Examine all the files that are run by cron and at. We've seen intruders leave back doors in files run from cron or submitted to at. These techniques can let the intruder back on the system even after you've kicked him/her off. Also, verify that all files/programs referenced (directly or indirectly) by the cron and at jobs, and the job files themselves, are not world-writable.

8) If your machine supports uucp, check the L.cmds file to see if they've added extra commands and that it is owned by root (not by uucp!) and world-readable. Also, the L.sys file should not be world-readable or world-writable.

-- --

9) Examine the /usr/lib/aliases (mail alias) file for unauthorized entries. Some alias files include an alias named 'uudecode'; if this alias exists on your system, and you are not explicitly using it, then it should be removed.

10) Look for hidden files (files that start with a period and are normally not shown by ls) with odd names and/or setuid capabilities, as these can be used to "hide" information or privileged (setuid root) programs, including /bin/sh. Names such as '.. ' (dot dot space space), '...', and .xx have been used, as have ordinary looking names such as '.mail'. Places to look include especially /tmp, /usr/tmp, and hidden directories (frequently within users' home directories).

11) Check the integrity of critical system programs such as su, login, and telnet. Use a known, good copy of the program, such as the original distribution media and compare it with the program you are running.

12) Older versions of systems often have security vulnerabilities that are well known to intruders. One of the best defenses against problems is to upgrade to the latest version of your vendor's system.

VMS SYSTEM ATTACKS:

13) The intruder exploits system default passwords that have not been changed since installation. Make sure to change all default passwords when the software is installed. The intruder also guesses simple user passwords. See point 1 above for suggestions on choosing good passwords.

14) If the intruder gets into a system, often the programs loginout.exe and show.exe are modified. Check these programs against the files found in your distribution media.

If you believe that your system has been compromised, contact CERT via telephone or email.

J. Paul Holbrook
Computer Emergency Response Team (CERT)
Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213-3890

Internet: cert@cert.sei.cmu.edu
Telephone: 412-268-7090 24-hour hotline: CERT personnel answer
7:30a.m.-6:00p.m. EST, on call for emergencies
other hours.

Past advisories and other information are available for anonymous ftp from cert.sei.cmu.edu (128.237.253.5).

References

Dalton90.
Dalton, J., ''Building a Constituency - An Ongoing Process,'' *Proceedings, Computer Emergency Response Team Workshop*, 1990.

Danca90.
Danca, R., ''Officials Confirm Latest Attempt to Invade Internet,'' *Federal Computer Week*, vol. 4, no. 12, 1990.

Denning90.
Denning, P., *Computers Under Attack*, ACM Press, 1990.

Fedeli90.
Fedeli, A., ''Forming and Managing a Response Team,'' *Proceedings, Computer Emergency Response Team Workshop*, 1990.

Graf90.
Graf, J., ''2 Charged With Illegal Computer Use,'' *Centre Daily Times*, February 17, 1990.

Alexander89.
Alexander, M., Johnson, M., ''Worm Eats Holes in NASA's Decnet,'' *Computer World*, October 23, 1989.

Markoff90a.
Markoff, J., ''3 Arrests Show Global Threat to Computers,'' *New York Times*, April 4, 1990.

Markoff90b.
Markoff, J., ''Student Says His Error Crippled Computers,'' *New York Times*, January 19, 1990.

Quarterman90.
Quarterman, J., *The Matrix: Computer Networks and Conferencing Systems Worldwide*, Digital Press, 1990.

Scherlis88.
Scherlis, W., ''DARPA Establishes Computer Emergency Response Team,'' *DARPA Press Release*, December 6, 1988.

Spafford88.
Spafford, E., ''The Internet Worm Program: An Analysis,'' Technical Report, Purdue University Department of Computer Sciences, 1988.

Stoll88.
Stoll, C., ''Stalking the Wily Hacker,'' *Communications of the ACM*, vol. 31, no. 5, 1988.

Stoll89.
Stoll, C., *The Cuckoo's Egg - Tracking a Spy Through the Maze of Computer Espionage*, Doubleday, 1989.