

CERT[®] System and Network Security Practices

Julia Allen

Systems, networks, and sensitive information can be compromised by malicious and inadvertent actions despite an administrator's best efforts. Even when administrators know what to do, they often don't have the time to do it; operational day-to-day concerns and keeping systems functioning take priority over securing those systems. Administrators need easy-to-access, easy-to-understand, easy-to-implement security practices. The CERT[®] system and network security practices are intended to meet those needs.

Editor's Note: This paper was presented at the NCISSE 2001: Fifth National Colloquium for Information Systems Security Education, held at George Mason University in Fairfax, VA, May 22-24, 2001. It will be published in the NCISSE proceedings. A longer version of this article is available online at http://www.cert.org/archive/pdf/NCISSE_practices.pdf.

The Problem as Viewed by Administrators

Administrators choose how to protect assets, but when managers are unable to identify the most critical assets and the nature of the threats against them (as part of a business strategy for managing information security risk), then the protections an administrator offers are likely to be arbitrary at best. Unfortunately, managers often fail to understand that securing assets is an ongoing process and not just a one-time fix. As a result, they do not consider this factor when allocating administrator time and resources. Even if an organization decides to outsource security services, it will probably continue to be responsible for the establishment and maintenance of secure configurations and the secure operations of critical assets.

Most system and network administrators only have their experience and well-meaning advice from peers to guide them in deciding how to protect and secure systems. They do not consult a published set of procedures that serve as de facto standards generally accepted by the administrator community because no such standards exist. Administrators are sorely in need of documented practices that are easy to access, understand, and implement. The practices summarized in this paper are intended to meet this need. They are fully described in my book *The CERT Guide to System and Network Security Practices*, recently published by Addison-Wesley (see <http://cseng.aw.com/book/0,,020173723X,00.html>).

[®] CERT and CERT Coordination Center are registered in the U.S. Patent and Trademark Office.

We recognize that it may not be practical to implement all steps within a given practice or even all practices. Business objectives, priorities, and an organization's ability to manage and tolerate risk dictate where information technology (IT) resources are expended and determine the tradeoffs among security and operational capability. However, by adopting these practices, an administrator can protect against today's threats, mitigate future threats, and improve the overall security of an organization's networked systems.

CERT Security Practices Structure

The CERT System and Network Security practices address 75 to 80 percent of the problems that are reported to the CERT/CC.¹ The practices describe the steps necessary to protect systems and networks from malicious and inadvertent compromise. Each practice consists of an introduction and a series of practical steps presented in the order of recommended implementation. There is also a section describing policy considerations (found in the practices on the CERT Web site at <http://www.cert.org/security-improvement/index.html?si>) that complements the steps and helps ensure that they will be deployed effectively.

All practices assume the existence of

- business objectives and goals from which security requirements derive. These may require periodically conducting an information-security risk analysis and assessment (such as the Organizationally Critical Threat, Asset, and Vulnerability EvaluationSM; see <http://www.cert.org/octave?si>) to help set priorities and formulate protection strategies.
- organization-level and site-level security policies that can be traced to the above business objectives, goals, and security requirements. If these security policies do not currently exist, developing them an essential task. Charles Cresson Wood, among others, has prepared an extensive reference guide describing all elements of a security policy along with sample policy language [Wood 2000].

Practices were written without reference to any one operating system or version. This makes the practice steps specific but still broadly applicable and ensures the practices will be useful and stay relevant longer than the most current version of an operating system. Examples of practice implementations specific to operating systems are available at the CERT Web site (<http://www.cert.org/security-improvement>).

¹ As determined by CERT vulnerability analysis and fourth quarter, 2000 incident analysis. In addition, the CERT security practices are periodically analyzed against top threat lists published by other organizations and consistently provide solutions for at least 80% of such threats.

SM Organizationally Critical Threat, Asset, and Vulnerability Evaluation and OCTAVE are service marks of Carnegie Mellon University.

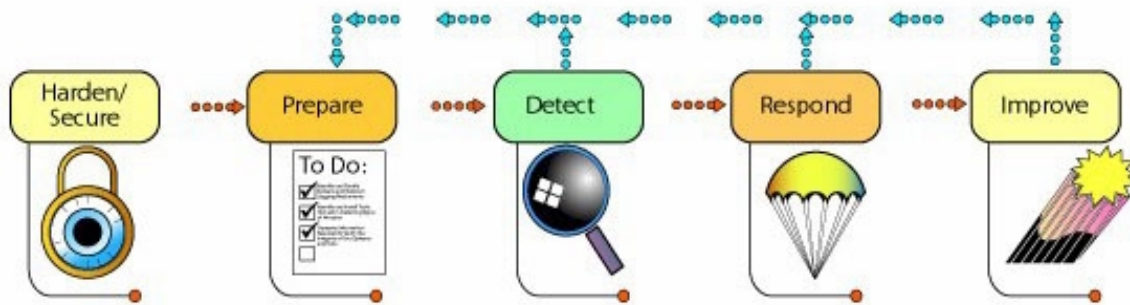


Figure 1: Steps for Securing Information Assets

Figure 1 above serves as a top-level depiction of how to secure and protect information assets. It includes steps to harden/secure, prepare, detect, respond, and improve.

The recommended practices to harden and secure systems form a strong foundation by securely configuring information assets (such as networks, systems, and critical data) and by establishing secure access to these assets. If this is done correctly *and maintained*, many of the common vulnerabilities used by intruders are eliminated. Following these practices can greatly reduce the success of many common, recurring attacks. Prepare, detect, respond, and improve practices assume that harden/secure practices have been implemented and provide further guidance about what to do when something suspicious, unexpected, or unusual happens.

Step One: Harden/Secure

Systems shipped by vendors are very usable but, unfortunately, often contain many weaknesses when viewed from a security perspective.² Vendors seek to sell systems that are ready to be installed and used by their customers. The systems come with most, if not all, services enabled by default. Vendors apparently want to minimize telephone calls to their support organizations and generally adopt a “one-size-fits-all” philosophy in relation to the systems they distribute. Therefore, an administrator must first redefine the system configuration to match the organization’s security requirements and policy for that system.

² Refer to the CERT vulnerability database (<http://www.kb.cert.org/vuls>), and the Common Vulnerabilities and Exposures (CVE) site (<http://cve.mitre.org>) for detailed vulnerability information.

This step will yield a hardened (secure) system configuration and an operational environment that protects against known attacks for which there are defined mitigation strategies. To complete this step, follow the instructions below in the order listed:

1. Install only the minimum essential operating system configuration—that is, only those packages containing files and directories that are needed to operate the computer.
2. Install patches to correct known deficiencies and vulnerabilities. Installing patches should be considered an essential part of installing the operating system but is usually conducted as a separate step.
3. Install the most secure and up-to-date versions of system applications. It is essential that all installations be performed before the next step (removing privileges) since any installation performed after privileges are removed can restore undesired access privileges.
4. Remove all privilege and access and then grant (add back in) privilege and access only as needed, following the principle “deny first, then allow.”
5. Enable as much system logging as possible to have access to detailed information (needed for in-depth analysis of an intrusion).

Practices for hardening and securing general-purpose network servers (NS) and user workstations (UW) are listed in Table 1 and are fully described on the CERT Web site [Allen 2000a, Simmel 99].

Plan	Address security issues in your computer deployment plan (NS, UW). Address security requirements when selecting servers (NS).
Configure	Keep operating systems and applications software up to date (NS, UW). Stick to essentials on the server host system (NS). Stick to essentials on the workstation host system (UW). Configure network service clients to enhance security (UW). Configure computers for user authentication (NS, UW). Configure operating systems with appropriate object, device, and file access controls (NS, UW). Configure computers for file backups (NS, UW). Use a tested model configuration and a secure replication procedure (UW).
Maintain	Protect computers from viruses and similar programmed threats (NS, UW). Configure computers for secure remote administration (NS, UW). Allow only appropriate physical access to computers (NS, UW).
Improve User Awareness	Develop and roll out an acceptable use policy for workstations (UW).

Table 1: Practices for Hardening and Securing Network Servers (NS=general-purpose network servers; UW=user workstations)

Additional hardening details can be found in the CERT document, *Installing and securing Solaris 2.6 servers*.³

Practices addressing more specific details for securing public Web servers (such as Web server placement, security implications of external programs, and using encryption) are listed in Table 2 and are documented on the CERT Web site [Kossakowski 2000].

Configure	<p>Isolate the Web server.</p> <p>Configure the Web server with appropriate object, device, and file access controls.</p> <p>Identify and enable Web-server specific logging mechanisms.</p> <p>Consider security implications for programs, scripts, and plug-ins.</p> <p>Configure the Web server to minimize the functionality of programs, scripts, and plug-ins.</p> <p>Configure the Web server to use authentication and encryption technologies.</p>
Maintain	Maintain the authoritative copy of your Web site content on a secure host.

Table 2: Practices for Securing Web Servers

Practices that provide guidance on deploying firewall systems (such as firewall architecture and design, packet filtering, alert mechanisms, and phasing new firewalls into operation) are listed in Table 3 and are presented on the CERT Web site [Fithen 99]. Public Web server and firewall practices assume that you have first configured a secure general-purpose server and have then built on it.

Prepare	Design the firewall system.
Configure	<p>Acquire firewall hardware and software.</p> <p>Acquire firewall training, documentation, and support.</p> <p>Install firewall hardware and software.</p> <p>Configure IP routing.</p> <p>Configure firewall packet filtering.</p> <p>Configure firewall logging and alert mechanisms.</p>
Test	Test the firewall system.
Deploy	<p>Install the firewall system.</p> <p>Phase the firewall system into operation.</p>

Table 3: Practices for Deploying Firewall Systems

³ Available at <http://www.cert.org/security-improvement> under UNIX implementations.

Step Two: Prepare

The philosophy of the preparation step hinges on the recognition that despite steps taken to harden and secure a system, there exist vulnerabilities yet to be identified. Consequently, an administrator must be able to recognize when these vulnerabilities are being exploited. To support such recognition, it is vitally important to characterize a system so that an administrator can understand how it works in a production setting. Through a thorough examination and recording of a known baseline state and expected changes at the network, system (including kernel), process, user, file, directory, and hardware levels, the administrator learns the expected behavior of an information asset. In addition, the administrator and his or her manager must develop policies and procedures to identify, install, and understand tools for detecting and responding to intrusions well before such policies, procedures, and tools need to be invoked.

One way to think about the distinction between the hardening and securing step and the characterization part of preparing is that hardening attempts to solve *known* problems by applying known solutions, whereas characterization helps administrators identify *new* problems and formulate new solutions. In the case of characterization, the problems are identified through anomaly-based detection techniques—that is, departures from normal behavior—so that new solutions can be formulated and applied.

Practices for characterizing information assets, preparing to detect signs of intrusion, and preparing to respond to intrusions are listed in Table 4 and are fully described on the CERT Web site [Allen 2000b, Kossakowski 99].

Define level of preparedness	Establish policies and procedures.
Implement preparation steps	Identify characterization and other data for detecting signs of suspicious behavior. Manage logging and other data collection mechanisms. Select, install, and understand tools for response.

Table 4: Practices for Characterizing Assets and Preparing for Intrusions

Step Three: Detect

This step occurs during the monitoring of transactions performed by some asset (such as looking at the logs produced by a firewall system or a public Web server). The administrator notices some unusual, unexpected, or suspicious behavior, learns something new about the asset's characteristics, or receives information from an external source (a user report, a call from another organization, a security advisory or bulletin). These indicate either that something should be

analyzed further or that something on the system has changed or should change (a new patch should be applied, a new tool version should be installed, etc). Analysis includes investigating unexpected or suspicious behavior that may be the result of an intrusion and drawing some initial conclusions, which are further refined during the **Respond** step. Possible changes include a number of improvement actions (see **Improve**, below) such as

- installing a patch (re-hardening)
- updating the configuration of a logging, data collection, or alert mechanism
- updating a characterization baseline to add unexpected but now acceptable behavior or remove no longer acceptable behavior
- installing a new tool

Practices are listed in Table 5 for detecting signs of intrusion in detection tools, networks, systems (including processes and user behavior), network and system performance, files and directories, hardware, and access to physical resources. These practices are fully described on the CERT Web site [Allen 2000b].

Integrity of intrusion detection software	Ensure that the software used to examine systems has not been compromised.
Behavior of networks and systems	Monitor and inspect network activities. Monitor and inspect system activities. Inspect files and directories for unexpected changes.
Physical forms of intrusion	Investigate unauthorized hardware attached to the network. Look for signs of unauthorized access to physical resources.
Follow through	Review reports of suspicious system and network behavior and events. Take appropriate actions.

Table 5: Practices for Detecting Signs of Intrusion

Step Four: Respond

In this step, an administrator further analyzes the damage caused by an intrusion (including the scope and effects of the damage), contains these effects as far as possible, works to eliminate future intruder access, and returns information assets to a known, operational state. It may be possible to do this step while continuing analysis.

Other parties that may be affected are notified, and evidence is collected and protected in case it is needed for legal proceedings against the intruder. Respond practices are listed in Table 6 and are described on the CERT Web site [Kossakowski 2000].

Handle	Analyze all available information. Communicate with relevant parties. Collect and protect information. Contain an intrusion. Eliminate all means of intruder access. Return systems to normal operation.
Improve	Implement lessons learned.

Table 6: Practices for Responding to Intrusions

Step Five: Improve

Improvement actions typically occur following a detection or response activity. In addition to those noted under **detect**, above, improvement actions may include

- further communicating with affected parties
- holding a post-mortem meeting to identify lessons learned
- updating policies and procedures
- updating tool configurations and selecting new tools
- collecting measures of resources required to deal with the intrusion and other security business-case information

Improvement actions may cause you to revisit harden/secure, prepare, and detect practices.

References

- [Allen 2000a] Allen, Julia. Kossakowski, Klaus-Peter. *Securing Network Servers* (CMU/SEI-SIM-010). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 2000. [Online] Available: <http://www.cert.org/security-improvement/modules/m10.html>.
- [Allen 2000b] Allen, Julia. Stoner, Ed. *Detecting Signs of Intrusion* (CMU/SEI-SIM-009). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 2000. [Online] Available: <http://www.cert.org/security-improvement/modules/m09.html>.
- [Fithen 99] Fithen, William, et al. *Deploying Firewalls*. (CMU/SEI-SIM-008). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1999. [Online] Available: <http://www.cert.org/security-improvement/modules/m08.html>.
- [Kossakowski 99] Kossakowski, Klaus-Peter, et al. *Responding to Intrusions* (CMU/SEI-SIM-006). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1999. [Online] Available: <http://www.cert.org/security-improvement/modules/m06.html>.
- [Kossakowski 2000] Kossakowski, Klaus-Peter. Allen, Julia. *Securing Public Web Servers* (CMU/SEI-SIM-011). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 2000. [Online] Available: <http://www.cert.org/security-improvement/modules/m11.html>.
- [Simmel 99] Simmel, Derek, et al. *Securing Desktop Workstations* (CMU/SEI-SIM-004). Pittsburgh, Pa.: Software Engineering Institute, Carnegie Mellon University, 1999. [Online] Available: <http://www.cert.org/security-improvement/modules/m04.html>.
- [Wood 2000] Wood, Charles Cresson. *Information Security Policies Made Easy Version 7*. Baseline Software, Inc., 2000.

About the Author

Julia Allen is a senior member of the technical staff within the Networked Systems Survivability Program at the Software Engineering Institute. The CERT[®] Coordination Center is also a part of this program. Allen is engaged in developing security-improvement practices for network-based systems. Prior to this technical assignment, Allen served as acting director of the SEI for an interim period of six months as well as deputy director/chief operating officer for three years. She started the Industry Customer Sector at the SEI in 1992.

Allen has more than 25 years of managerial and technical experience in software engineering. Before joining the SEI, she held the position of vice president at Science Applications International Corporation (SAIC), where she was responsible for starting a new software division specializing in embedded systems software for government customers. She was at SAIC for eight years. Allen also spent 10 years at TRW in Redondo Beach, CA., where her work included a range of assignments from integration, test, and field site support to managing major software-development programs.

She received a BS in computer science from the University of Michigan, an MS in electrical engineering from the University of Southern California, and an executive business certificate from the University of California at Los Angeles (UCLA). Her professional affiliations include ACM and IEEE Computer Society.

Allen's publications include Security for Information Technology Service Contracts (CMU/SEI-SIM-003, 1998); Responding to Intrusions (CMU/SEI-SIM-006, 1999), Deploying Firewalls (CMU/SEI-SIM-008, 1999), Detecting Signs of Intrusion (CMU/SEI-SIM-009, 2000), Securing Network Servers (CMU/SEI-SIM-010, 2000), Securing Public Web Servers (CMU/SEI-SIM-011, 2000); six reports within the Security Improvement module series; State of the Practice in Intrusion Detection Technologies (CMU/SEI-99-TR-028); *The CERT Guide to System and Network Security Practices* (Addison-Wesley, June 2001); and various presentations and papers on the CERT security practices, intrusion detection systems, and the SEI's strategic plan and technical program.

The Software Engineering Institute (SEI) is a federally funded research and development center sponsored by the U.S. Department of Defense and operated by Carnegie Mellon University.

® CMM, Capability Maturity Model, Capability Maturity Modeling, Carnegie Mellon, CERT, and CERT Coordination Center are registered in the U.S. Patent Trademark Office.

SM ATAM; Architecture Tradeoff Analysis Method; CMMI; CMM Integration; CURE; IDEAL; Interim Profile; OCTAVE; Operationally Critical Threat, Asset, and Vulnerability Evaluation; Personal Software Process; PSP; SCAMPI; SCAMPI Lead Assessor; SCE; Team Software Process; and TSP are service marks of Carnegie Mellon University.

TM Simplex is a trademark of Carnegie Mellon University.