CERTÒ[1] System and Network Security Practices[i]

Julia Allen
Carnegie Mellon University
Software Engineering Institute
Networked Systems Survivability Program, CERT Coordination Center

This paper was presented at the NCISSE 2001: 5th National Colloquium for Information Systems Security Education, held at George Mason University in Fairfax, VA on May 22-24, 2001. It will be published in the NCISSE proceedings.

Abstract: Networks have become indispensable for conducting business in government, commercial, and academic organizations. Networked systems allow you to access needed information rapidly, improve communications while reducing their cost, collaborate with partners, provide better customer services, and conduct electronic commerce. While computer networks revolutionize the way you do business, the risks they introduce can be fatal to a business. Attacks on networks can lead to lost money, time, products, reputation, sensitive information, and even lives.

Systems, networks, and sensitive information can be compromised by malicious and inadvertent actions despite an administrator’s best efforts. Even when an administrator knows 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.

The knowledge that most system and network administrators have about protecting and securing systems typically comes from experience and word-of-mouth, not by consulting a published set of procedures that serve in the role of de facto standards generally accepted by the administrator community; these do not currently exist. For this reason and others described in this paper, an administrator needs easy-to-access, easy-to-understand, easy-to-implement security practices. The CERT system and network security practices are intended to meet these needs.

CERT security practices are organized into five top-level steps: Harden/Secure, Prepare, Detect, Respond, and Improve. A total of fifty current practices comprise these steps. They are summarized in this paper and fully documented on the CERT web site at http://www.cert.org. The practices to harden and secure systems form a strong foundation by establishing secure configurations of computing assets. Prepare, Detect, Respond, and Improve practices assumes that Harden/Secure practices have been implemented and provide further guidance on what to do when something suspicious, unexpected, or unusual occurs.

[1] CERT and CERT/CC are registered in the U.S. Patent and Trademark Office.

CERT System and Network Security Practices[2]

I. The Problem – In The Large[3]

Networks have become indispensable for conducting business in government, commercial, and academic organizations. Networked systems allow you to access needed information rapidly, improve communications while reducing their cost, collaborate with partners, provide better customer services, and conduct electronic commerce.

Many organizations have moved to distributed, client-server architectures where servers and workstations communicate through networks. At the same time, they are connecting their networks to the Internet to sustain a visible business presence with customers, partners, and suppliers. While computer networks have revolutionized the way companies do business, the risks they introduce can be devastating. Attacks on networks can lead to lost money, time, products, reputation, sensitive information, and even lives.

The 2000 Computer Security Institute/FBI Computer Crime and Security Survey [1] indicates that the number of computer crime incidents and other information security breaches is still rising and that the cost of the damage they cause is increasing. For example, 70 percent of the 585 respondents reported computer security breaches within the twelve months previous to the 2000 survey — an increase from 62 percent reported in the 1999 survey. Furthermore, the total financial losses for the 273 organizations that were able to quantify them added up to $265,586,240 — more than doubling the reported losses from the 1999 figure of $123,779,000.

Engineering for ease of use is not being matched by engineering for ease of secure administration. More and more people are using the power of new software and computers to work with greater effectiveness and efficiency. Most products are so easy to use that people with little technical knowledge or skill can install complex software and run it on their desktop computers. Unfortunately, it is difficult to configure and operate many of these products securely. This gap between the knowledge needed to operate a system and that needed to keep it secure is resulting in increasing numbers of vulnerable systems. [2]

Technology evolves so rapidly that vendors concentrate on reducing the time it takes to bring a new product to market, often trying to save time spent in product development by placing a low priority on building in security features. Until their customers demand products that are more secure, the situation is unlikely to change.

Users count on their systems working properly when they need them and assume, to the extent that they think about it, that their Information Technology (IT) departments are operating all systems securely. But this may not be the case.

[2] The material in this article is taken largely from the book *The CERT$^{\text{Ò}}$ Guide to System and Network Security Practices*, published by Addison-Wesley in June 2001.

[3] This Problem description is directly quoted from an article in Crosstalk magazine. [3].

System and network administrators typically have insufficient time, knowledge, and skill to keep today's complex systems and networks running smoothly and consistently. Also, evolving attack methods and emerging software vulnerabilities continually introduce new threats into an organization's technology and systems. Thus, even vigilant, security-conscious organizations discover that security starts to degrade almost immediately after fixes, workarounds, and new technology are put in place. Inadequate security in the IT infrastructures can negatively affect the integrity, confidentiality, and availability of systems and data.

Because of the rapid expansion of Internet use, the demand for workers qualified in computer security far exceeds the supply. The shortage applies to both those in formal degree programs and those who have acquired their knowledge and skills through experience. As a result, people who are not properly qualified are being hired or promoted from within to take care of system and network security. This trend is exacerbated by the fact that some skilled, experienced system administrators change jobs frequently to increase their salaries or switch to a less stressful type of job because of burnout.

Who has this problem? The answer is just about everyone—anyone who uses information technology infrastructures that are networked, distributed, and heterogeneous needs to care about improving the security of networked systems.

Whether you acknowledge it or not, your organization's networks and systems are vulnerable to both internal and external attack. Organizations cannot conduct business and build products without a robust IT infrastructure. An IT infrastructure vulnerable to intruder attack cannot be robust. In addition, users have an organizational, ethical, and often legal responsibility to protect sensitive data or information that would help competitors. They must also preserve the reputation of their organizations and business partners. All of these can be severely compromised by successful intrusions.

II. The Problem – As Viewed by Administrators

Systems, networks, and sensitive information can be compromised by malicious or inadvertent actions despite an administrator's best efforts. Even when administrators know what to do, they often don't have the time to take action; operational day-to-day concerns and the need to keep systems functioning take priority over securing those systems.

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 learned about how to protect and secure systems from experience and from well-meaning advice from peers, not by consulting a published set of procedures that serve as de facto standards generally accepted by the administrator community. No such standards currently exist. For these reasons, administrators are sorely in need of security practices that are easy to access, understand, and implement. The practices described in this paper are intended to meet these needs.

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 IT resources are expended and determine the trade-offs among security and function, operational capability, and capacity. However, we believe that by adopting these practices, an administrator can act now to protect against today’s threats, mitigate future threats, and improve the overall security of the organization’s networked systems.

III. CERT Security Practices Structure

We chose the topics addressed by the CERT practices and defined their scope to address 75 to 80 percent of the problems that are reported to the CERT/CC[4]. 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) 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 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 is recognized as an essential task and is progressing. Charles Cresson Wood [4], among others, has prepared an extensive reference guide describing all elements of a security policy along with sample policy language.

[4] 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.

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).

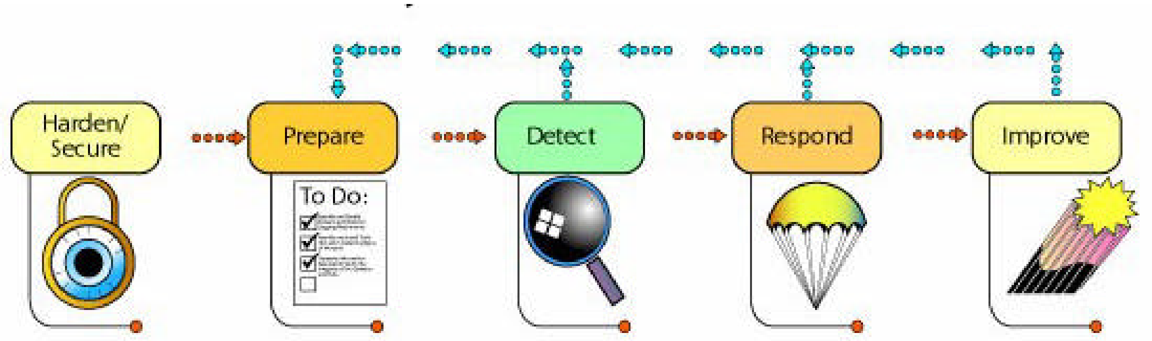

Figure 1 above serves as a top-level depiction of how to secure and protect information assets. It includes steps to Harden/Secure, Prepare, Detect, Respond, and Improve.

The recommended practices to harden and secure systems form a strong foundation by establishing secure configurations of and access to information assets (networks, systems, critical data, etc.). 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.

A. Harden/Secure

Systems shipped by vendors are very usable but unfortunately, often contain many weaknesses when viewed from a security perspective. [5] This idea is depicted as Swiss cheese in Figure 1. Vendors seek to sell systems that are ready to be installed and used by their customers. The systems perform as advertised, and they 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 needs to first redefine the system configuration to match the organization’s security requirements and policy for that system.

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:

[5] 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.

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, as any installation performed after privileges are removed can undo such removal and results in, for example, changed mode bits or added accounts.

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 in the case of 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 [5] & [6].

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 Rollout an Acceptable Use Policy for Workstations (UW)

Table 1

Additional hardening details can be found in the CERT implementation *Installing and securing Solaris 2.6 servers.*[6]

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 documented on the CERT web site [7].

Configure	Isolate the Web Server Configure the Web Server with Appropriate Object, Device, and File Access Controls Identify and Enable Web-Server-Specific Logging Mechanisms Consider Security Implications for Programs, Scripts, and Plug-ins Configure the Web Server to Minimize the Functionality of Programs, Scripts, and Plug-ins Configure the Web Server to Use Authentication and Encryption Technologies
Maintain	Maintain the Authoritative Copy of Your Web Site Content on a Secure Host

Table 2

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 presented on the CERT web site [8]. Public web server and firewall practices assume that you have first configured a secure general-purpose server and then built on it.

Prepare	Design the Firewall System
Configure	Acquire Firewall Hardware and Software Acquire Firewall Training, Documentation, and Support Install Firewall Hardware and Software Configure IP Routing Configure Firewall Packet Filtering Configure Firewall Logging and Alert Mechanisms
Test	Test the Firewall System
Deploy	Install the Firewall System Phase the Firewall System into Operation

Table 3

B. Prepare

The philosophy of the preparation step hinges on the recognition that there exists a collection of vulnerabilities yet to be identified. This requires an administrator to be in a position to recognize when these vulnerabilities are being exploited. To support such

[6] Available at http://www.cert.org/security-improvement under UNIX implementations.

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 of 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 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 fully described on the CERT web site [9] & [10].

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

C. 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 stimulus (a user report, a call from another organization, a security advisory or bulletin). These indicate either that something needs to be analyzed further or that something on the system has changed or needs to change (a new patch needs to be applied, a new tool version needs to 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-harden)
- 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 [9].

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

D. 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 the event it should be needed for legal proceedings against the intruder. Respond practices are listed in Table 6 and described on the CERT web site [7].

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

E. 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

[1] Computer Security Institute, "2000 CSI/FBI Computer Crime and Security Survey," *Computer Security Issues and Trends*, vol. VI, no. 1, Spring 2000.

[2] Pethia, Richard. "Internet Security Issues: Testimony before the U.S. Senate Judiciary Committee." Carnegie Mellon University, Software Engineering Institute, May 25, 2000. [Online] Available: http://www.cert.org/congressional_testimony/ Pethia_testimony25May00.html.

[3] Allen, Julia, et al. "Improving the Security of Networked Systems." *Crosstalk: The Journal of Defense Software Engineering, Vol. 13 No. 10*. October, 2000. [Online] Available: http://www.stsc.hill.af.mil/Crosstalk/crostalk.html.

[4] Wood, Charles Cresson. *Information Security Policies Made Easy Version 7*. Baseline Software, Inc., 2000.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[i] A presentation on this topic can be found on the CERT/CC web site at http://www.cert.org/archive/ppt/NCISSE.ppt