

Securing Information Assets

Julia Allen

“Thousands of Computer Networks Compromised,” “Customer Credit Card Numbers Posted on the Web,” “Government Web Site Defaced Again,” “Email Attachment Delivers Destructive Payload.” How many times have we read headlines like this in the last year? People who attack computer networks and systems are determined to leave their mark, steal data, or break into your system for a host of other reasons. Many malicious intruders are armed with sophisticated tools and knowledge of the latest computer vulnerabilities. How can we stop them?

The Networked Systems Survivability program at the SEI is dedicated to finding solutions for keeping networked systems secure. Networked systems and the sensitive information they contain can be compromised despite an administrator’s best efforts. Even when administrators know they should be devoting more time to security, they often cannot: keeping systems functioning takes priority over securing those systems. Administrators need a clear and comprehensive set of security practices that are easy to find and follow.

The CERT® system and network security practices represent more than fifty best practices to address all phases of securing systems and networks. CERT security practices are organized into five broad groupings based on the order in which they are performed. They are

- Harden and secure
- Prepare to detect and respond to intrusions
- Detect intrusions
- Respond to intrusions
- Improve

The complete set of practices is available on the CERT Web site at <http://www.cert.org/security-improvement/index.html>. Also, this summer Addison-Wesley will publish a book entitled *The CERT Guide to System and Network Security Practices*, written by Julia Allen of the SEI.

Figure 1 illustrates how to secure and protect information assets (such as a network or Web server) using the CERT security practices.

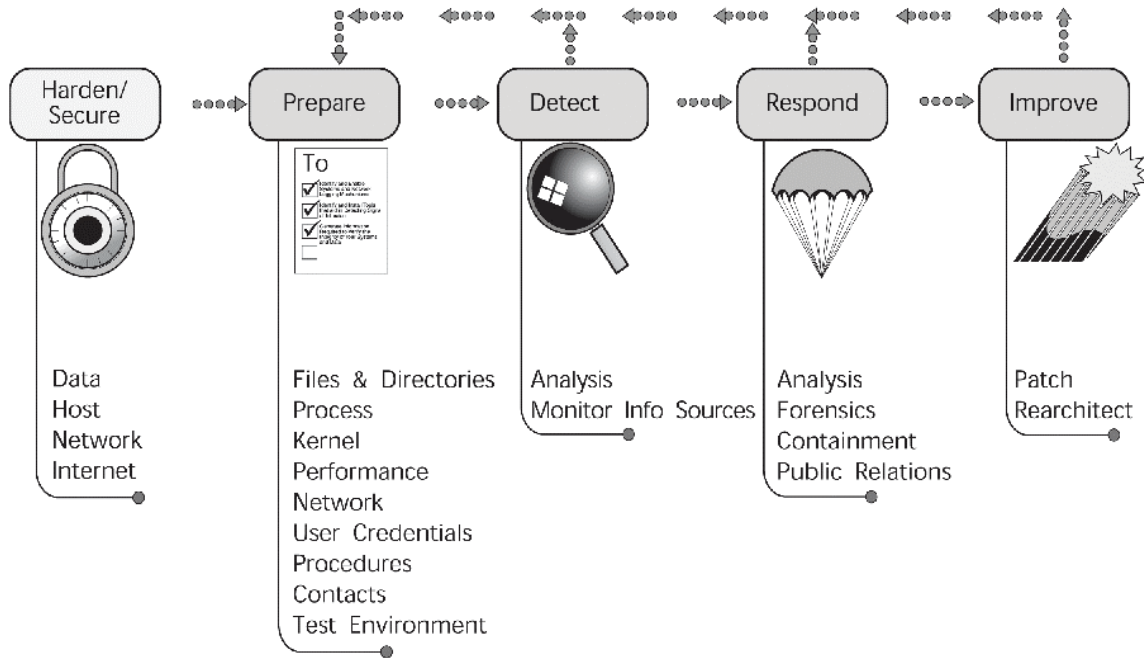


Figure 1: The Structure of CERT Security Practices

The CERT practices were created to address 75 to 80 percent of the problems that are reported to the CERT Coordination Center (CERT/CC) at the SEI. The practices do not make reference to any one operating system or version, so the principles will remain valid despite the rapid advances in technologies. However, many practices are linked to documents called implementations that do discuss specific operating systems and software. Implementations are available from <http://www.cert.org/security-improvement/#implementations>.

The Five Steps

1. Harden and Secure

Systems shipped by vendors are very usable but, unfortunately, often contain many security weaknesses. This step yields a hardened (secure) system configuration and an operational environment that protects against known attacks for which there are designated mitigation strategies.

2. Prepare to Detect and Respond to Intrusions

This step starts with the assumption that there are many vulnerabilities not yet identified. An administrator must be able to recognize when an unknown vulnerability is being exploited. How can an administrator recognize what is not there? The major method to help recognize exploitation is to characterize a system so that an administrator can understand how it works in a production setting. Then, any deviations will provide the clue to noticing unexpected or suspicious activity.

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 they need to be invoked.

3. Detect Intrusions

This step occurs when an administrator is monitoring system or network transactions by, for example, 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).

4. Respond to Intrusions

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 much 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.

5. Improve

Administrators also need to take action to improve their systems following detection or response activities. In addition to practices contained in the step Detect Intrusions, improvement actions may include

- further communicating with affected parties
- holding a post mortem meeting to discuss 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

Even when system administrators know how to secure systems, they often don't have the time to take action. The CERT security practices, organized into five top-level steps, provide administrators with guidance that is easy to access, understand, and implement.

For more information, contact—

Customer Relations

Phone

412 / 268-5800

Email

customer-relations@sei.cmu.edu

World Wide Web

<http://www.cert.org/security-improvement/index.html>

Copyright © 2001 Carnegie Mellon University

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.