Securing Information Assets: Security Knowledge in Practice

Lawrence Rogers and Julia Allen
Software Engineering Institute

System and network administrators are an organization's first lines of defense in protecting critical information assets. They need a framework for organizing and selecting security practices that are easy to understand, describe, and implement. The authors propose the Security Knowledge in Practice (SKiP) method as a solution.

Critical information assets (systems, networks, and sensitive data) can be compromised by malicious or inadvertent actions despite an organization's best efforts. System and network administrators are on the firing line and even when they know what to do, they often do not 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 must choose how to protect assets. But when managers cannot prioritize critical assets and threats (as part of a business strategy for managing information security risk), then the protections an administrator offers will be arbitrary at best. Unfortunately, managers often fail to understand that securing assets is an ongoing process. They do not consider this factor when allocating administrator time and resources.

Most system and network administrators learned from their peers how to protect and secure systems, not by consulting published procedures that serve as de facto standards accepted by the administrator community – no such standards currently exist. Administrators are sorely in need of a structure for organizing, prioritizing, and selecting security practices that is easy to understand, describe, justify, and implement.

Tackling the Problem

The Security Knowledge in Practice (SKiP℠)[1] method was developed to organize security practices published on the Computer Emergency Response Team (CERT®)/CERT Coordination Center® Web site into a more process-based approach, departing from the more common problem-based approach. SKiP defines a cyclical process for establishing and sustaining the security of critical information assets such as the following:

- Systems running mission critical applications.
- Network infrastructure, including routers, hubs, and switches.

Due to space constraints, CrossTalk *was not able to publish this article in its entirety. However, it can be viewed in this month's issue on our Web site at <www.stsc.hill.af.mil/crosstalk> along with back issues of* CrossTalk.