© Route66 | Dreamstime.com

Managing Security: The Security Content Automation Protocol

Shirley Radack and Rick Kuhn, *National Institute of Standards and Technology*

Managing information systems security is an expensive and challenging task. Many different and complex software components—including firmware, operating systems, and applications—must be configured securely, patched when needed, and continuously monitored for security. Most organizations have an extensive set of security requirements. For commercial firms, such requirements are established through complex interactions of business goals, government regulations, and insurance requirements; for government organizations, security requirements are mandated.

Meeting these requirements has been time consuming and error prone, because organizations have lacked standardized, automated ways of performing the tasks and reporting on results. They've also lacked interoperability across security tools. Using proprietary names for vulnerabilities or platforms, for example, creates inconsistencies in reports from multiple tools that can cause organizational delays in carrying out security assessments, decision making, and vulnerability remediation.

To overcome these deficiencies and reduce security administration costs, the National Institute of Standards and Technology developed the Security Content Automation Protocol (http://scap.nist.gov) using community-supported security resources. SCAP (pronounced "ess-cap") is a suite of specifications that standardizes the format and nomenclature by which security software products communicate information about software identification, software flaws, and security configurations. This multipurpose protocol supports automated vulnerability checking, technical control compliance activities, and security measurement.

Standardizing System Security Reporting

SCAP was designed to organize, express, and measure security-related information in standardized ways, using standard reference data, such as identifiers for post-compilation software flaws and security configuration issues. SCAP can help maintain the security of enterprise systems by automatically verifying the installation of patches, checking system security configuration settings, and examining systems for signs of compromise. Organizations must manage the security of many different systems, applications, and operating systems that have different mechanisms for patching and managing security configuration. The same software often needs to be secured somewhat differently on multiple hosts.

Another issue is the need to reconfigure software or install patches when vulnerabilities are discovered or attackers target a system. Priorities must be established to quickly address the most important vulnerabilities. When vulnerability scanners don't use standardized names, the security staff might not know whether the different scanners are reporting on the same vulnerabilities. SCAP's standardized, automated methods let organizations manage these time-consuming and error-prone processes and overcome the lack of interoperability among different security tools.

Organizations can also use SCAP to demonstrate compliance with the requirements established

1520-9202/11/$26.00 © 2011 IEEE

Table 1. Current Security Content Automation Protocol (SCAP) specifications.

Category	Specification	Definition
Language	eXtensible Configuration Checklist Description Format (XCCDF)	An XML specification for structured collections of security configuration rules used by operating system (OS) and application platforms.
	Open Vulnerability and Assessment Language (OVAL)	An XML specification for exchanging technical details on how to check systems for security-related software flaws, configuration issues, and patches.
Enumeration	Common Platform Enumeration (CPE)	A naming convention for hardware, OS, and application products.
	Common Configuration Enumeration (CCE)	A dictionary of names for software security configuration issues, such as access-control and password-policy settings.
Vulnerability	Common Vulnerabilities and Exposures (CVE)	A dictionary of names for publicly known security-related software flaws.
	Common Vulnerability Scoring System (CVSS)	A method for classifying characteristics of software flaws and assigning severity scores based on these characteristics.

by the US government. Furthermore, SCAP complies with

- INCITS/ISO/IEC 27001, an international standard specifying the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving information security management systems;
- Department of Defense Directive 8500, which establishes information assurance requirements; and
- the Federal Information System Controls Audit Manual.

Individual specifications that compose SCAP can also be used for forensic activities and other purposes. SCAP doesn't replace other security software, and support for SCAP can be incorporated into existing software.

Technical Specifications

SCAP specifications are grouped into three categories (see Table 1):

- languages for specifying checklists, generating checklist reports, and specifying the low-level testing procedures that the checklists use;
- enumerations, which include nomenclatures and dictionaries for security and product-related information; and
- vulnerability measurement and scoring systems, which measure the characteristics of vulnerabilities and generate scores based on those characteristics.

SCAP uses standard reference data to identify software flaws and security configurations. This reference data, also known as *SCAP content*, is provided by the National Vulnerability Database (managed by NIST and sponsored by the Department of Homeland Security).

Adopting SCAP

How can organizations use SCAP to manage security-related information in standardized ways?

Standardize Security Configuration Checklists

A security configuration checklist expressed using SCAP documents the desired security configuration settings, installed patches, and other system security elements in a standardized format. Organizations can obtain SCAP-expressed checklists for their systems' software from the NIST Configuration Checklist Program (http://checklists.nist.gov) and customize them as appropriate to meet specific organizational requirements.

Although the current version of SCAP can't automatically implement checklists, SCAP-expressed checklists can be applied using proprietary methods. Organizations can use SCAP-expressed checklists on an ongoing basis to confirm that systems are configured properly.

Demonstrate Compliance

SCAP-expressed checklists can map individual system security configuration settings to their corresponding high-level security requirements. The configuration identifiers are embedded in SCAP-expressed checklists, which let SCAP-enabled tools automatically generate assessment and compliance evidence when combined with the mapping reference data. This increased automation can significantly reduce the effort needed to achieve assessment results, providing substantial cost savings.

For information about mapping security configuration settings to the security controls, see http://nvd.nist.gov/cce.cfm.

Use Standardized Enumerations

Organizations use a collection of tools for security management, such as vulnerability scanners, patch management utilities, and intrusion detection systems. SCAP lets organizations use standardized enumerations when referring to security-related software flaws, security configuration issues, and platforms. The common understanding achieved using standardized enumerations makes it easier to use security tools, share information, and provide guidance to address security issues.

Security software vendors have moved quickly to support the Common Vulnerabilities and Exposures (CVE), Common Configuration Enumeration (CCE), and Common Platform Enumeration (CPE) in their products. Including CVE and CCE identifiers and CPE product names in vulnerability and patch advisories makes it easier for organizations to use these resources efficiently.

Measure Vulnerability

SCAP lets organizations quantitatively and repeatedly measure and score software flaw vulnerabilities across systems using the Common Vulnerability Scoring System (CVSS), CVE, and CPE (see http://nvd.nist.gov). The ability to accurately and consistently convey vulnerability characteristics lets organizations institute consistent and repeatable mitigation policies throughout the enterprise.

Organizations can use CVSS base scores to help prioritize the remediation of known security-related software flaws according to the flaws' relative severity. CVSS scores can be used more easily when organizations use CVE to reference specific vulnerabilities. When a new vulnerability is publicly announced, NIST creates a new CVE for it, identifies the affected products using CPE, and computes the CVSS base measures and score. This information is then added to the National Vulnerability Database. Organizations can review the CVSS base measures and scores for each new CVE as part of their processes to prioritize and mitigate vulnerabilities. They can also use SCAP content to check systems for the new vulnerability.

The SCAP Validation Program

Under the Security Content Automation Protocol (SCAP) validation program, independent laboratories are accredited by the NIST National Voluntary Laboratory Accreditation Program. These laboratories conduct defined tests on information system security products and submit a test report and relevant results to NIST. Based on the independent laboratory's test report, the SCAP validation program then validates the product under test. See http://nvd.nist.gov/scapproducts.cfm for a list of validated products.

Acquire SCAP-Validated Products

The SCAP product validation program (http://scap.nist.gov/validation) helps ensure that SCAP products are thoroughly tested and validated to conform to SCAP requirements. The program emphasizes a modular component architecture such that SCAP-validated products are interoperable and interchangeable. It also focuses on correctness testing where appropriate, such as for vulnerability and configuration scanning.

Many acquisition officials have included requirements for SCAP-validated products in their procurements. For example, the US Office of Management and Budget requires federal agencies and agency IT providers to use SCAP-validated Federal Desktop Core Configuration (FDCC) scanners for testing and assessing FDCC compliance. (For more information, see the sidebar.)

Integrate SCAP with Software Products

Many software products can now assess the underlying software configuration settings using SCAP, instead of relying on manual checks or proprietary checking mechanisms. Also, product vendors and other checklist developers often create their checklists using SCAP and contribute to the National Checklist Program to promote the widespread availability of the checklists.

Security automation is challenging because it often involves thousands of software products and deals with a threat environment that literally changes every day. SCAP is making it possible for business and government organizations to automate an ever-growing portion of their security management tasks to save both time and money.

Acknowledgment

This article was adapted from "Security Content Automation Protocol: Helping Organizations Maintain and Verify the Security of their Information Systems," NIST ITL Bulletin, *Sept. 2010, by Shirley Radack. Any mention of commercial products or reference to commercial organizations is for information only; it doesn't imply recommendation or endorsement by NIST, nor does it imply that the products mentioned are necessarily the best available for the purpose.*

***Shirley Radack** is a guest researcher at the US National Institute of Standards and Technology. Contact her at shirley.radack@nist.gov.*

***Rick Kuhn** is a computer scientist at the US National Institute of Standards and Technology. Contact him at kuhn@nist.gov.*