Managing Security Using 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, established for commercial firms through complex interactions of business goals, government regulations, and insurance requirements, and which are mandated by statute for government organizations. In the past, meeting these requirements has been time-consuming and error-prone because there have been no standardized, automated ways of performing all of the tasks and reporting on results. Another obstacle has been the lack of interoperability across security tools. For example, using proprietary names for vulnerabilities or platforms creates inconsistencies in reports from multiple tools, and this incompatibility can cause organizational delays in carrying out security assessments, decision-making, and vulnerability remediation activities.

To overcome these deficiencies and reduce security administration costs, the Security Content Automation Protocol (SCAP) was developed by NIST, using community-supported security resources such as the Common Vulnerabilities and Exposures specification. Pronounced "ess-cap," SCAP is a suite of specifications that standardize the format and nomenclature by which security software products communicate information about software identification, software flaws, and security configurations. A multipurpose protocol, SCAP supports automated vulnerability checking, technical control compliance activities, and security measurement.

How SCAP Helps Organizations Manage Security and Comply With Reporting Requirements

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 be used to 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 and when systems are targeted by attackers. Priorities must be established to assure that the most important vulnerabilities are addressed quickly. When vulnerability scanners do not use standardized names for vulnerabilities, the security staff may be unsure whether the different scanners are reporting on the same vulnerabilities.

The standardized, automated methods provided by SCAP enable organizations to manage these time-consuming and error-prone processes, and to overcome the lack of interoperability among different security tools. SCAP can be used to demonstrate compliance with the requirements established by the US government, as well as other requirements: for example, 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 (DOD) Directive 8500, establishing information assurance requirements; and the Federal Information System Controls Audit Manual (FISCAM). Individual specifications that comprise SCAP can also be used for forensic activities and other purposes. SCAP does not replace other security software, and support for SCAP can be incorporated into existing software.

Technical Specifications for SCAP

SCAP specifications are grouped into three categories: (1) languages for specifying checklists, generating checklist reports, and specifying the low-level testing procedures used by the checklists; (2) enumerations that include nomenclatures and dictionaries for security and product-related information; and (3) vulnerability measurement and scoring systems for measuring the characteristics of vulnerabilities and generating scores based on those characteristics. The current specifications are:

· eXtensible Configuration Checklist Description Format (XCCDF), an Extensible Markup Language (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;

· 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 settings, password policy settings;

· Common Vulnerabilities and Exposures (CVE™), a dictionary of names for publicly known security-related software flaws; and

· Common Vulnerability Scoring System (CVSS), a method for classifying characteristics of software flaws and assigning severity scores based on these characteristics.

(OVAL, CCE, CPE, and CVE are trademarks of The MITRE Corporation. XCCDF and SCAP are trademarks of NIST.)

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

Adopting and Using SCAP

How can organizations use SCAP to manage security-related information in standardized ways? Here are some approaches:

• **Using security configuration checklists that are expressed using SCAP to improve and monitor the security of systems**.

A security configuration checklist that is expressed using SCAP (an SCAP-expressed checklist) 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, and then customize the checklists as appropriate to meet specific organizational requirements. While the current version of SCAP does not provide a capability to 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.

• Using SCAP to demonstrate compliance with high-level security requirements that originate from mandates, standards, and guidelines.

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 allow SCAP-enabled tools to 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.

Information about the mapping of security configuration settings to the security controls is available at http://nvd.nist.gov/cce.cfm.

• **Using standardized SCAP enumerations—identifiers and product names.**

Organizations frequently use a collection of tools for security management, such as vulnerability scanners, patch management utilities, and intrusion detection systems. SCAP allows organizations to use standardized enumerations when referring to security-related software flaws, security configuration issues, and platforms. The common understanding achieved through the use of 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.

- **Using SCAP for vulnerability measurement and scoring.**

SCAP enables quantitative and repeatable measurement and scoring of software flaw vulnerabilities across systems through the combination of the Common Vulnerability Scoring System (CVSS), CVE, and CPE. The ability to accurately and consistently convey vulnerability characteristics allows organizations to institute consistent and repeatable mitigation policies throughout the enterprise. Organizations can use CVSS base scores to assist in prioritizing the remediation of known security-related software flaws based on the relative severity of the flaws. CVSS scores can be used more easily when organizations use CVE to reference specific vulnerabilities. When a new vulnerability is publicly announced, a new CVE identifier is created for it, the affected products are identified using CPE, and the CVSS base measures and score are computed and 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. SCAP content can be used to check systems for the presence of the new vulnerability.

- **Acquiring and using SCAP-validated products.**

The SCAP product validation program helps to ensure that SCAP products are thoroughly tested and validated to conform to SCAP requirements. The validation program emphasizes a modular component architecture such that SCAP-validated products are interoperable and interchangeable. The validation program 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, OMB requires federal agencies and agency IT providers to use SCAP-validated Federal Desktop Core Configuration (FDCC) scanners for testing and assessing FDCC compliance.

- **Integrating SCAP with software products.**

Many software products now are capable of assessing the underlying software configuration settings using SCAP, rather than 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.

The SCAP Validation Program

The SCAP Validation Program tests products for the capability to use the features and functionality available through SCAP. Under the SCAP Validation Program, independent laboratories are accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP). 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. A list of validated products is publicly available.

Conclusions

Security automation is challenging because of the extent of the problem, often involving thousands of software products, and 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 in a way that saves time and money for the organizations.

Online resources for SCAP include:

- SCAP program - http://scap.nist.gov
- SCAP Validation Program - http://scap.nist.gov/validation
- National Checklist Program - http://checklists.nist.gov
- National Vulnerability Database - http://nvd.nist.gov

Disclaimer

This article was abridged and 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 does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.