ITL BULLETIN FOR JANUARY 2012

ADVANCING SECURITY AUTOMATION AND STANDARDIZATION: REVISED TECHNICAL SPECIFICATIONS ISSUED FOR THE SECURITY CONTENT AUTOMATION PROTOCOL (SCAP)

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
U.S. Department of Commerce

The Security Content Automation Protocol (SCAP) is a suite of specifications that standardize the format and nomenclature by which software products communicate information about software flaws and security system configurations, both to machines and humans. Pronounced "ess-cap," SCAP is a multipurpose suite of specifications that support automated checking of security configuration settings, vulnerability checking, technical control compliance activities, and security measurement.

SCAP was developed through the cooperation and collaboration of public and private sector organizations, including government, industry and academia. In conducting business, organizations must manage many different and complex software components, including firmware, operating systems and applications. These components must be configured securely, patched when needed, and continuously monitored for security. The components must be able to interact safely and securely to deter widespread cyber attacks and to deal with any attacks that might occur. The use of standardized, automated methods for system security management can help organizations operate more effectively in complex, interconnected environments and realize cost savings, an asset in today's fiscally constrained situations.

Many organizations, including the federal government, are adopting SCAP and encouraging its use to implement the automation of security activities. SCAP is also being adopted by major software manufacturers and is becoming a significant component of large information security management and governance programs. Both users and suppliers of software components have a common interest in achieving open specifications for security automation and system security management. Standardized specifications promote the interoperability of security products and create opportunities for product innovation.

The Information Technology Laboratory at the National Institute of Standards and Technology (NIST) has been working with other organizations to develop technical specifications for SCAP. Recently NIST issued an updated specification as Special Publication 800-126 Rev. 2, *The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2.* The publication defines the technical composition of SCAP version 1.2, including its component specifications, their interrelationships and interoperation, and the requirements for SCAP content.

NIST Special Publication (SP) 800-126 Rev. 2, The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2

Written by David Waltermire and Stephen Quinn of NIST, Karen Scarfone of Scarfone Cybersecurity, and Adam Halbardier of Booz Allen Hamilton, SP 800-126 Revision 2 defines and explains SCAP version 1.2, and defines requirements for creating and processing SCAP source content. These requirements build on the previous SCAP revisions and the requirements defined within individual SCAP component specifications, enabling new ways to build SCAP content. SCAP version 1.2 also provides specifications for digital signing of content to support content and result integrity, for asset identification, and for new assessment methods. SCAP version 1.2 incorporates eleven component specifications that are detailed below.

Sections of the publication discuss the high-level requirements that must be met for conformance with the SCAP version 1.2 specification; the requirements and recommendations for SCAP content syntax, structure, and development; SCAP content processing requirements and recommendations; and content requirements and recommendations for particular use cases. Technical details are presented in tables and figures. The appendices to the report include an overview of major security considerations for SCAP implementation; acronym and abbreviation lists; a glossary of terms used; references and other resources; and a list of changes that were made to drafts of the specification.

SP 800-126 Rev. 2 is available at
http://csrc.nist.gov/publications/nistpubs/800-126-rev2/SP800-126r2.pdf.

Components of SCAP Version 1.2

SCAP version 1.2 includes eleven component specifications in five categories:

• **Languages**. The SCAP languages provide standard vocabularies and conventions for expressing security policy, technical check mechanisms, and assessment results. The SCAP language specifications are:

· Extensible Configuration Checklist Description Format (XCCDF) 1.2, a language for authoring security checklists/benchmarks and for reporting results of evaluating them;
· Open Vulnerability and Assessment Language (OVAL) 5.10, a language for representing system configuration information, assessing machine state, and reporting assessment results; and
· Open Checklist Interactive Language (OCIL) 2.0, a language for representing checks that collect information from people or from existing data stores made by other data collection efforts.

• **Reporting formats.** The SCAP reporting formats provide the necessary constructs to express collected information in standardized formats. The SCAP reporting format specifications are:

· Asset Reporting Format (ARF) 1.1, a format for expressing the transport format of information about assets and the relationships between assets and reports; and
· Asset Identification (AI) 1.1, a format for uniquely identifying assets based on known identifiers and/or known information about the assets.

• **Enumerations.** Each SCAP enumeration defines a standard nomenclature (naming format) and an official dictionary or list of items expressed using that nomenclature. The SCAP enumeration specifications are:

· Common Platform Enumeration (CPE) 2.3, a nomenclature and dictionary of hardware, operating systems, and applications names;
·Common Configuration Enumeration (CCE) 5, a nomenclature and dictionary of software security configuration identifiers; and
·Common Vulnerabilities and Exposures (CVE), a nomenclature and dictionary of security-related software flaw identifiers.

• **Measurement and scoring systems.** These systems evaluate specific characteristics of a security weakness, such as software vulnerabilities and security configuration issues, and generate a score that reflects their relative severity. The SCAP measurement and scoring system specifications are:

· Common Vulnerability Scoring System (CVSS) 2.0, a system for measuring the relative severity of software flaw vulnerabilities; and
· Common Configuration Scoring System (CCSS) 1.0, a system for measuring the relative severity of system security configuration issues.

• **Integrity.** The SCAP integrity specification helps to preserve the integrity of SCAP content and results. The SCAP integrity specification is:

· Trust Model for Security Automation Data (TMSAD).

See the **For More Information** section below for references that explain these specifications.

NIST Recommendations for Applying SCAP

NIST recommends that organizations developing content or products based on SCAP version 1.2 adopt the following practices:

• **Follow the requirements listed in SP 800-126 and in the associated component specifications.** Organizations should ensure that their implementation and use of SCAP version 1.2 comply with the requirements detailed in each component specification and the overall technical specification. Conflicts in requirements between different component specifications are clarified in NIST SP 800-126. The requirements specified in NIST SP 800-126 should be used if there is a conflict between the component specifications and NIST SP 800-126.

•**When creating SCAP content, adhere to the conventions specified in NIST SP 800-126.** Security products and checklist authors assemble content from SCAP data repositories to create SCAP-conformant security guidance. For example, a security configuration checklist can document desired security configuration settings, installed patches, and other system security elements using a standardized SCAP format. Such a checklist would use XCCDF to describe the checklist, CCE to identify security configuration settings to be addressed or assessed, and CPE to identify platforms for which the checklist is valid. The use of CCE and CPE entries within XCCDF checklists is an example of an SCAP convention and is a requirement for valid SCAP usage.

These conventions are considered part of the definition of SCAP version 1.2. Organizations producing SCAP content should adhere to these conventions to ensure the highest degree of interoperability. NIST provides an SCAP Content Validation Tool that organizations can use to help validate the correctness of their SCAP content. The tool checks that SCAP source and result content is well-formed, all cross-references are valid, and required values are appropriately set. For details, see http://scap.nist.gov/revision/1.2/#tools.

Community Participation in the Development of SCAP

SCAP was developed through the cooperation and collaboration of public and private sector organizations. Interested parties from industry, research and educational institutions, and government are working to advance automation and standardization of technical security operations. Information about email-based discussion lists, conferences, and technical working groups sponsored by a variety of organizations, as well as general information about the SCAP program, is available from the web page http://scap.nist.gov/.

Validation of SCAP Products

The SCAP Validation Program tests the capability of products to use the features and functionality available through SCAP and its component standards. Under the SCAP Validation Program, independent laboratories are accredited by the NIST National Voluntary Laboratory Accreditation Program (NVLAP) to conduct tests that are developed by NIST. The laboratories test products in accordance with the test requirements and deliver the results to NIST. The SCAP Validation Program validates the product under test, based on the independent laboratory test report. The validations

that have been awarded for vendor products are posted on the NIST SCAP Validated Products web page at http://nvd.nist.gov/scapproducts.

The current test requirements document, NIST Interagency Report (IR) 7511 Rev. 3, *Security Content Automation Protocol (SCAP) Version 1.2 Validation Program Test Requirements*, is being updated to include test requirements based on SCAP version 1.2. The revision will provide a test suite to assist product vendors in the development of their products, and enable end users to conduct their own testing. Accredited third-party laboratories will be able to use these new requirements and expanded test suites to ensure greater product and content interoperability. Detailed information concerning the draft updated test requirements is available at http://csrc.nist.gov/publications/drafts/nistir-7511/Draft-nistir-7511_R3.pdf.

Future Activities

NIST will continue to detail the specific and appropriate usage of the SCAP version 1.2 components and their interoperability, and to encourage the creation of reliable SCAP content and the development of a wide array of SCAP products.

SCAP is expected to evolve and expand in support of the growing needs to define and measure effective security controls, assess and continuously monitor ongoing aspects of information security, and successfully manage systems. Risk management methods, such as the Risk Management Framework (RMF) developed by NIST, help organizations balance the operational and economic costs of protective measures for their information and information systems with the gains in capabilities and improved support of organizational missions resulting from the use of efficient protection procedures.

NIST is also leveraging SCAP as part of a continuous monitoring technical reference model that provides detailed specifications to enable product interoperability and inter-organizational information sharing between different systems within the enterprise environment. Implementations of this model will support collecting data from across a diverse set of security tools, data analytics and scoring, user queries, and overall situational awareness. The model is designed so organizations can meet these goals by leveraging their existing SCAP investments.

For more information on the RMF and the continuous monitoring reference model, see the **For More Information** section below.

Many different security activities and disciplines can potentially benefit from standardized expression and reporting. Areas include compliance, remediation, and network monitoring. NIST encourages contributions and participation in developing these additional techniques.

The federal government will continue to support public and private partnerships to develop, maintain, and implement voluntary consensus standards for cybersecurity best

practices. Widely accepted standards that are implemented in products are needed to protect the interoperability, security, and resilience of the global infrastructure.

For More Information

SCAP utilizes software flaw and security configuration standard reference data. 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). See the NIST web page http://nvd.nist.gov/.

NIST maintains the National Checklist Repository (NCR), a publicly available resource that contains information on a variety of security configuration checklists for specific IT products or categories of IT products. The repository contains checklists (and pointers to tools) for performing configuration checking of systems implementing the United States Government Configuration Baseline (USGCB) and the Federal Desktop Core Configuration (FDCC), both using SCAP. The NCR also hosts pointers to other SCAP-enabled checklists produced by IT product vendors and government organizations. Information about the NCR is available at http://web.nvd.nist.gov/view/ncp/repository.

To achieve adequate security, federal managers must actively manage the risks to their core missions and business functions, and to the information and information systems supporting those missions and functions. NIST developed the Risk Management Framework (RMF) to guide agencies through a structured process to identify the risks to the information systems, assess the risks, and take steps to reduce risks to an acceptable level. The RMF is available at http://csrc.nist.gov/groups/SMA/fisma/index.html.

Some of the NIST publications that support the implementation of SCAP include:

Draft NIST Special Publication (SP) 800-117 Revision 1, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP)*, provides an overview of SCAP Version 1.2, presents SCAP at a conceptual level, focusing on how organizations can use SCAP-enabled tools to enhance their security posture. It also explains to IT product and service vendors how they can adopt SCAP version 1.2 capabilities within their offerings.

NIST SP 800-51 Revision 1, *Guide to Using Vulnerability Naming Schemes*, advises organizations on the use of the vulnerability naming schemes: Common Vulnerabilities and Exposures (CVE) and Common Configuration Enumeration (CCE). The publication also advises software and service vendors on how they should use vulnerability names and naming schemes in their product and service offerings.

NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, guides federal agencies in selecting and specifying security controls for information systems to meet the requirements of Federal Information Processing Standard (FIPS) 200, *Minimum Security Requirements for Federal Information and Information Systems.*

NIST Interagency Report (NISTIR) 7275 Revision 4, *Specification for the Extensible Configuration Checklist Description Format (XCCDF) Version 1.2*, is the latest revision of an Extensible Markup Language (XML)-based model that enables the standardized expression of security configuration rules. XCCDF provides a uniform foundation for expression and compliance assessment of security checklists and other configuration guidance, and thereby advances more widespread application of sound security practices. XCCDF 1.2 supports SCAP version 1.2.

NISTIR 7802, *Trust Model for Security Automation Data 1.0 (TMSAD)*, helps users to establish integrity, authentication, and traceability for security automation data. Since security automation data is primarily stored and exchanged using Extensible Markup Language (XML) documents, the focus of the trust model is on the processing of XML documents. The trust model is composed of recommendations on how to use existing specifications to represent signatures, hashes, key information, and identity information in the context of an XML document within the security automation domain.

Additional continuous monitoring reference model publications include:

Draft NISTIR 7756, *CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Model*, provides a reference model for organizations to collect data from across a diverse set of security tools, analyze the data, score the data, enable user queries, and provide overall situational awareness. The model is designed to help organizations meet these goals by leveraging their existing security tool investments and avoiding designing and paying for custom solutions. It was developed using the Department of Homeland Security (DHS) continuous monitoring framework named Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) architecture as a starting point.

Draft NISTIR 7799, *Continuous Monitoring Reference Model Workflow, Subsystem, and Interface Specifications*, provides the technical specifications for the continuous monitoring reference model presented in draft NISTIR 7756 with enough specificity to enable instrumentation of existing products and development of new capabilities by vendors. The specifications in draft NISTIR 7799 define an ecosystem in which a variety of interoperable products can be combined into a continuous monitoring solution.

Draft NISTIR 7800, *Applying the Continuous Monitoring Technical Reference Model to the Asset, Configuration and Vulnerability Management Domains*, augments the reference model with guidance on addressing these specific areas. It leverages the Security Content Automation Protocol (SCAP) version 1.2 for configuration and vulnerability-scan content, and it specifies reporting results in an SCAP-compliant format.

For information about NIST standards and guidelines, and related publications, see the NIST web page http://csrc.nist.gov/publications/index.html.

Information about NIST's information security programs is available from the Computer

Security Resource Center at http://csrc.nist.gov.

ITL Bulletin Publisher: Elizabeth B. Lennon
Writer/Editor, Information Technology Laboratory
National Institute of Standards and Technology
elizabeth.lennon@nist.gov