Security Automation from a NIST Perspective

by John Banghart, Stephen Quinn, and Kevin Stine

Security automation can harmonize the vast amounts of information technology (IT) data into coherent, comparable information streams that inform timely and active management of diverse IT systems. Through the creation of internationally recognized, flexible, and open standards, security automation can facilitate IT infrastructure interoperability and broad acceptance and adoption and create opportunities for innovation.

As part of the larger security automation initiative, the Security Content Automation Protocol (SCAP) provides standardized data models and methods for assessing and reporting vulnerability and configuration state of computing systems.

SCAP 1.2

SCAP continues to evolve to meet the needs of expanding use cases, and the security automation community continues to work on refining the capabilities it provides.

Although SCAP has enabled the successful implementation of some limited use cases including the Federal Desktop Core Configuration (FDCC)/ United States Government Configuration Baseline (USGCB) initiative, the significantly greater potential of SCAP is realized with the advent of SCAP 1.2. What is this potential? From a configuration and vulnerability scanning perspective, it means having plentiful SCAP content for commonly used computing operating systems and applications that interoperate seamlessly with validated products that can process and produce correct results and work aggressively to continue wide-scale use and adoption.

SCAP 1.2 Feature Set

SCAP 1.2 builds on previous versions of SCAP by introducing a method for integrating underlying specifications *via* a cohesive data stream model, allowing practitioners to build SCAP content using the primitive specifications in new and innovative ways not defined in the comprising specifications. SCAP 1.2 also introduces digital signing of content to ensure content and result integrity, specifications for asset identification and reporting, and support for new assessment methods using PowerShell. SCAP 1.2 also makes it possible to assess a hybrid of operating system, application, and artifact targets using a single data stream by dynamically determining at runtime the settings and system state rather than be beholden to a static list of settings (as with previous versions of SCAP).

SCAP Validation

To ensure that commercially available security products are able to correctly use SCAP 1.2, the SCAP Validation program was expanded to include new requirements and much more robust testing capabilities. Working closely with National Security Agency (NSA) and Department of Homeland Security (DHS), in the fall of 2011, National Institute of Standards and Technology (NIST) will introduce an updated set of Derived Test Requirements based on SCAP 1.2 along with a publically available test suite that will assist product vendors in the development of their products and provide end user organizations with the ability to conduct their own testing. In keeping with the existing process, accredited third-party laboratories will use these new requirements and significantly expanded test suites to ensure greater product and content interoperability.

SCAP Use Cases

Continuous Monitoring

Information security continuous monitoring enables an organization to maintain ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

The process of continuously monitoring the security of systems throughout an enterprise is challenging for several reasons. Most organizations have large heterogeneous computing environments that consist of numerous

operating systems and applications that require secure configuration and patch management. Keeping up with the demands of daily operations while also demonstrating compliance with security requirements expressed in legislation, regulation, and policy is challenging without a proper strategy that involves security automation.

Organization-wide information security continuous monitoring can be difficult using manual processes alone. The use of SCAP checklists and validated products for assembling organization-wide information security information can facilitate efficiencies and improve effectiveness. Recent additions to SCAP 1.2 ensure security automation will expand to still additional use cases within this highly important problem space.

Secure System Configurations

Another supporting use case for continuous monitoring is the USGCB for Windows 7, Internet Explorer 8, and Red Hat Enterprise Linux, representing an evolution from the earlier FDCC for Windows XP, Windows Vista, and Internet Explorer 7. [1] After consulting with the Chief Information Officer (CIO) Council agencies, the Technology Infrastructure Sub-committee (TIS) of the Federal CIO Council took the important lessons from the implementation of the FDCC on federal desktop systems and has put forth a true baseline for Windows 7 and Red Hat Enterprise Linux 5. As with the FDCC, the USGCB checklists use SCAP as the basis for the machine-readable policy. In the future, the TIS will leverage National Checklist Program-hosted checklists at Tier III ranking for inclusion as future USGCB candidates for federal use and adoption. [2]

Health IT

The application of security automation principles and specifications are being extended beyond the federal government to provide value across other sectors and within the context of additional security frameworks.

Security automation is being leveraged to assist healthcare organizations in improving their ability to enable measurement and monitoring of security controls and configurations and to support security compliance management with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (45 CFR 160, 162, and 164). [3]

By leveraging the FDCC and USGCB initiatives described earlier, NIST is using SCAP specifications to develop HIPAA-specific baseline security configuration checklists for common operating systems that host electronic health record systems, enabling greater automation of the HIPAA Security Rule technical safeguards.

A prototype HIPAA Security Rule self-assessment application, containing nearly 1,000 questions expressed using the Open Checklist Interactive Language, will help HIPAA covered entities and other healthcare organizations to better understand the HIPAA Security Rule standards and safeguards and assist in implementing and assessing those standards and safeguards in their operational environments.

International Standardization

The United States Government (USG) recognizes the benefit of a U.S. public and private partnership to develop, maintain, and implement voluntary consensus standards related to cybersecurity best practices to ensure the interoperability, security, and resiliency of this global infrastructure. This position is supported and guided by U.S. legislation and policy and is illustrated by the USG's promotion and assistance over the past two decades to advance security in commercial off-the-shelf IT products. [4] It has also become widely accepted by the USG and many others that standards only provide value if they are widely used.

Industry has shown great interest in incorporating SCAP into their products but would like to take advantage of

economies of scale and ensure that the products they design and produce can be sold globally in multiple markets and validated against one set of standards.

This condition will arise only if SCAP and its supporting components, as well as other specifications in the security automation body of work, are accepted by foreign governments and other major global market players. In turn, many foreign governments and major players are more likely to accept SCAP validated products and not develop their own similar standards if SCAP and its supporting components are accepted and further developed within an acceptable international standards development organization.

Outreach

Broad community involvement and adoption of security automation technologies has always been a hallmark of this multi-year initiative. In addition to open mailing lists and Web sites, several events take place throughout the course of the year to bring experts together to advance the state-of-the-art in security automation. The Security Automation Developer Days is a multi-day event that is the primary face-to-face venue for experts to discuss and approve changes or additions to SCAP and other security automation specifications.

The Software Assurance (SwA) Program of the DHS's National Cyber Security Division co-sponsors SwA Forums semi-annually with organizations in the Department of Defense and NIST. [5] The purpose of the forums is to bring together members of the government, industry, and academia with vested interests in SwA to discuss and promote integrity, security, and reliability in software.

Once a year, NIST, DHS, and NSA sponsor the IT Security Automation Conference to give end users from the government and industry an opportunity to learn about how security automation can assist them in meeting their missions and give them the opportunity to interact directly with experts and hear from senior leaders on where security automation is headed.

These activities ensure that the government and industry are able to coordinate the use cases, resources, and technologies necessary to improve cybersecurity through standards and automation.

Looking Forward

While SCAP has achieved some success and continues to evolve to address new needs, it is not intended to solve all the cybersecurity challenges with which we are faced. To expand the goals of security automation further, NIST and its government and industry partners are conducting research and development into new areas. One such area is network event management, called the Event Management Automation Protocol (EMAP). These specifications bring the successful model of SCAP to the network event space, providing standardized methods for classifying event data and how it is communicated, filtered, correlated, and prioritized. EMAP will provide a level of data and tool interoperability that is required for dealing with the vast numbers of events being generated everyday by desktops, servers, routers, firewalls, *etc.*

Security automation has been and continues to be a broad and active effort that brings together the government and industry to solve real cybersecurity challenges today. Security automation lays the groundwork for solving the cybersecurity challenges of tomorrow through the development of best practices, technical standardization, and international adoption. ■

Disclaimer: Certain commercial equipment, instruments, or materials are identified in this report to adequately specify the experimental procedure. Such identification does not imply recommendation or endorsement by the NIST nor does it imply that the materials or equipment identified are necessarily the best available for the purpose.

About the Authors

John Banghart, Stephen Quinn, and Kevin Stine support the NIST Information Technology Laboratory (ITL) Computer Security Division (CSD). The NIST ITL CSD provides standards and technology to protect information systems against threats to the confidentiality of information, integrity of information and processes, and availability of information and services in order to build trust and confidence in Information Technology (IT) systems.

References

1. *http://usgcb.nist.gov*
2. *http://checklists.nist.gov*
3. The HIPAA Security Rule establishes national standards to protect individuals' electronic protected health information that is created, received, used, or maintained by a covered entity by requiring appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.
4. The "National Technology Transfer and Advancement Act" and "Office of Management and Budget (OMB) Circular A-119 Revised: Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities.
5. *https://buildsecurityin.us-cert.gov/swa/index*