New version of security automation protocol includes digital trust model

July 20 2011

Researchers at the National Institute of Standards and Technology (NIST) have released for public comment updated specifications for the Security Content Automation Protocol (SCAP), which helps organizations find and manage computer-system vulnerabilities more effectively by standardizing the way vulnerabilities are identified, prioritized and reported.

SCAP unites and organizes a collection of computer security specifications and reference data to support automated security programs that check vulnerabilities in information systems, such as configuration errors, missing software "patches," misapplied security settings and many others. SCAP-based security tools are particularly valuable for securing large, complex information systems and organizations with many distributed computing systems.

System operations and security professionals use SCAP-based software products to determine the system's status, particularly information about software flaws and security configuration information in an efficient, accurate way. For example, SCAP enables automated assessment of software patches present on a system that identifies the potential security risk to an organization due to an unpatched vulnerability. Using SCAP, information system administrators can address critical vulnerabilities mitigating the risk of attack.

In The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2 (NIST Special Publication 800-126

Revision 2) some underlying specifications have been enhanced in response to requests from SCAP content authors and product developers. SCAP has been updated to incorporate three new underlying specifications to the protocol that add asset reporting, asset identification and a digital trust model to help ensure the integrity of SCAP data itself.

The digital trust model in SP 800-126 Rev. 2 is described in the draft NIST Interagency Report 7802: Trust Model for Security Automation Data 1.0. The model has applications beyond the security automation environment. It permits users to establish integrity, authentication and traceability of security automation XML data using a 21st century version of a 17th century king's wax seal on a scroll. The trust model is based on existing specifications from the World Wide Web Consortium and describes features that will enhance the trustworthiness of information.

The U.S. federal government employs SCAP to support security activities and initiatives. Academia and private industry, such as finance, manufacturing and health care, also use the protocol as it provides a standardized situational awareness view of IT systems that can be used by system administrators, security officers and executives to make security decisions.

SCAP is expected to evolve and expand to support the growing needs to define and measure effective security controls, assess and monitor ongoing aspects of information security, and successfully manage systems in accordance with risk management frameworks such as NIST SP 800-53, Department of Defense Instruction 8500.2, and the Payment Card Industry (PCI) framework.

More information: The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.2 (NIST Draft Special Publication 800-126 Revision 2) can be found at

csrc.nist.gov/publications/dra … raft-SP800-126r2.pdf . Trust Model for Security Automation Data 1.0 can be found at csrc.nist.gov/publications/dra … raft-nistir-7802.pdf .

Provided by National Institute of Standards and Technology