Security Content Automation Protocol Progress Report

presented by:
Tim Grance
National Institute of Standards and Technology

Agenda

- Current State Summary
- Security Content Automation Protocol Primer
- Vendor Opportunity
- FISMA Compliance
- What's This Mean for Me
- Current and Near-Term Use Cases
- Current State
- Near and Long Term Vision

Current State Summary

A Study in Cause and Effect

Governing Bodies

Recognize the need to improve security and mandate it in an increasing number of laws, directives, and policies

Standards Bodies

Try to keep pace with an increasing number of mandates by generating more frameworks and guidelines

Product Teams

Based on the increasing number of mandates, see the need for automation, many seek to enable it through proprietary methods

Service Providers

Based on the increasing number of mandates, see the need for automation and have responded by 1) learning a wide variety of both open and proprietary technologies and 2) implementing point solutions

Operations Teams

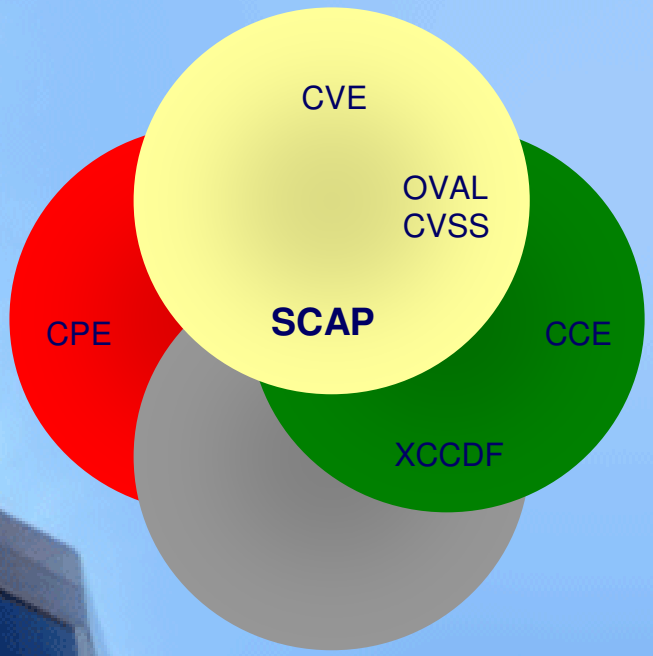
Lacking true automation, 1) have become overwhelmed by an increasing number of mandates, frameworks, and guidelines and 2) are spending a considerable amount of resources trying to keep pace

What is SCAP?

How

Standardizing the format by which we communicate

Protocol



What

Standardizing the information we communicate

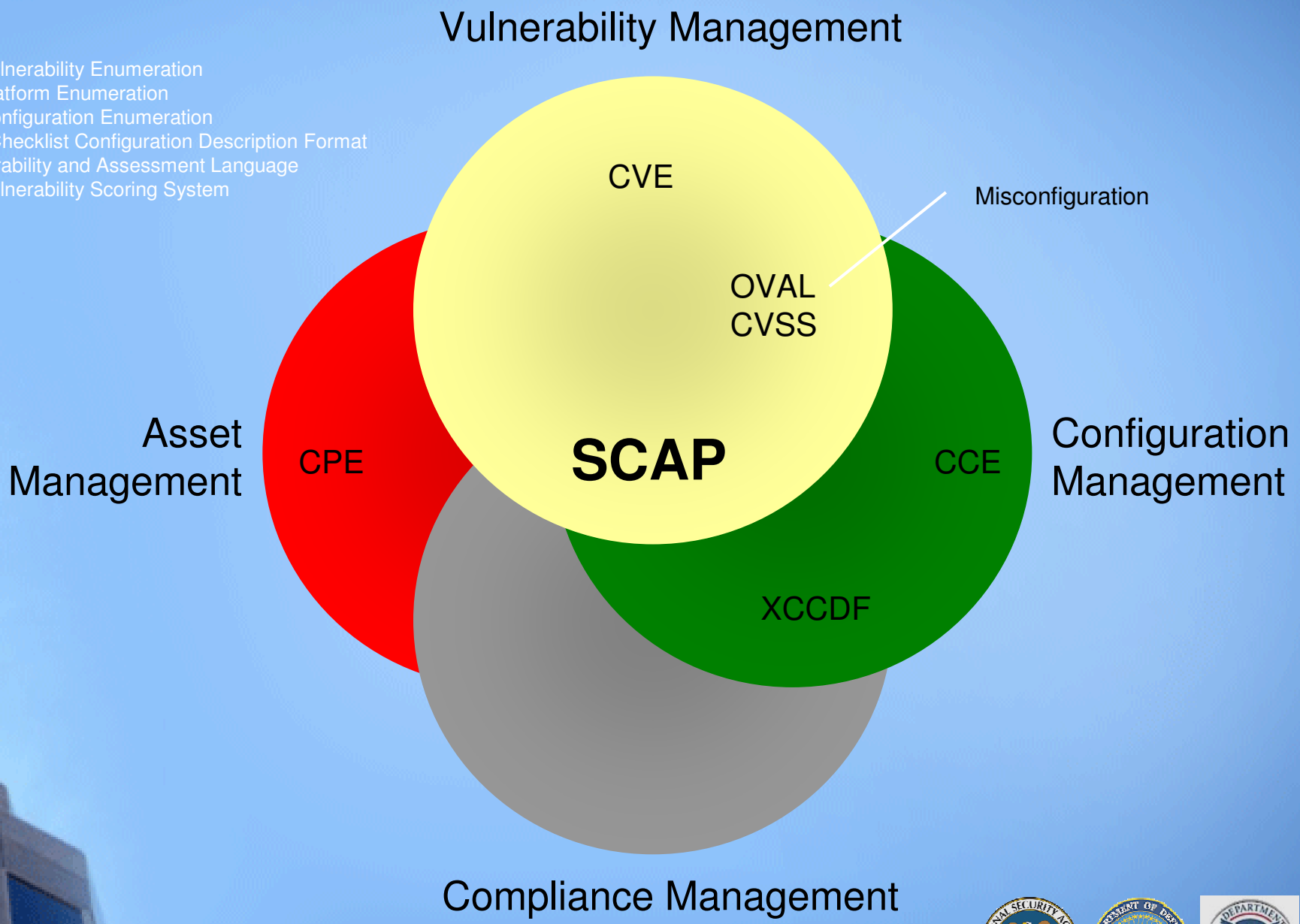
Content

http://nvd.nist.gov

- 50 million hits per year
- 20 new vulnerabilities per day
- Mis-configuration cross references
- Reconciles software flaws from US CERT and MITRE repositories
- Produces XML feed for NVD content

Integrating IT and IT Security Through SCAP

Common Vulnerability Enumeration
Common Platform Enumeration
Common Configuration Enumeration
eXtensible Checklist Configuration Description Format
Open Vulnerability and Assessment Language
Common Vulnerability Scoring System



SCAP Value

Feature	Benefit
Standardizes ***how*** computers communicate vulnerability information – the protocol	▪Enables interoperability for products and services of various manufacture
Standardizes ***what*** vulnerability information computers communicate – the content	▪Enables repeatability across products and services of various manufacture ▪Reduces content-based variance in operational decisions and actions
Based on open standards	▪Harnesses the collective brain power of the masses for creation and evolution ▪Adapts to a wide array of use cases
Uses configuration and asset management standards	▪Mobilizes asset inventory and configuration information for use in vulnerability and compliance management
Applicable to many different Risk Management Frameworks – Assess, Monitor, Implement	▪Reduces time, effort, and expense of risk management process
Detailed traceability to multiple security mandates and guidelines	▪Automates portions of compliance demonstration and reporting ▪Reduces chance of misinterpretation between Inspector General/auditors and operations teams
Keyed on NIST SP 800-53 security controls	▪Automates portions of FISMA compliance demonstration and reporting

Federal Risk Management Framework

Starting Point

FIPS 199 / SP 800-60

Categorize Information System

Define criticality /sensitivity of information system according to potential impact of loss

FIPS 200 / SP 800-53

Select Security Controls

Select baseline (minimum) security controls to protect the information system; apply tailoring guidance as appropriate

SP 800-53 / SP 800-30

Supplement Security Controls

Use risk assessment results to supplement the tailored security control baseline as needed to ensure adequate security and due diligence

SP 800-18

Document Security Controls

Document in the security plan, the security requirements for the information system and the security controls planned or in place

SP 800-70

Implement Security Controls

Implement security controls; apply security configuration settings

SP 800-53A

Assess Security Controls

Determine security control effectiveness (i.e., controls implemented correctly, operating as intended, meeting security requirements)

SP 800-37

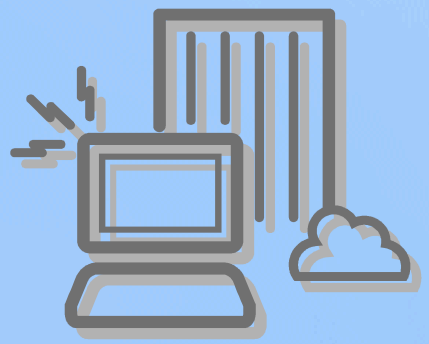
Authorize Information System

Determine risk to agency operations, agency assets, or individuals and, if acceptable, authorize information system operation

SP 800-37 / SP 800-53A

Monitor Security Controls

Continuously track changes to the information system that may affect security controls and reassess control effectiveness



Controls with Automated Validation Support

Tool Set	Automation	Control Count	Control Percent	Control Example
Framework Tools	Full Automation	-	-	-
	Partial Automation	49	30%	PL-2 System Security Plan
Security Content Automation Protocol	Full Automation	31	19%	AC-11 Session Lock
	Partial Automation	39	24%	AC-8 System Use Notification
Future Automation Techniques		44	27%	AC-1 Access Control Policy and Procedures
	Total Controls	163	100%	

What's This Mean to Me

Activity	Benefit
Product Teams	
Continue authoring checklists, hardening guidelines, and security configurations in SCAP format	▪Ensure that all parties check your security settings using the most direct method ▪Obtain National Checklist Program logo
Continue adoption of all SCAP standards	▪Increase revenue - consumer recognition of product enabling interoperability with related disciplines like asset, configuration, and compliance management ▪Increase opportunity - ability to expand into asset, configuration, and compliance management tool markets
Put SCAP technologies on your roadmap and budget accordingly	▪Enable interoperability, repeatability, automation
Service Providers	
Continue authoring checklists, hardening guidelines, and security configurations in SCAP format	▪Obtain National Checklist Program logo
Prepare to help the operations community reconcile multiple mandates into XCCDF checklists	▪Enable reuse between Federal customers
Position yourself to integrate SCAP capable products	▪Support Federal compliance with OMB memorandum M-07-18 and the 31 July 2007 memo to the CIOs
Put SCAP and vulnerability management automation on your services roadmap and budget accordingly	▪Enable interoperability, repeatability, automation

What's This Mean to Me

Activity	Benefit
Operations Teams	
Interact with your vendors and service providers about SCAP, ask about their SCAP plans, ask about their SCAP readiness	▪Set expectations
Consider phrasing like "SCAP capable" in your acquisition language	▪Ensure compliance with OMB memorandum M-07-18 (FDCC) and the 31 July 2007 (SCAP/FDCC) memo to the CIOs
Put SCAP and vulnerability management automation on your roadmap and budget accordingly	▪Enable interoperability, repeatability, automation

Stakeholder and Contributor Landscape: Industry

Product Teams and Content Contributors

Stakeholder and Contributor Landscape: Federal Agencies

SCAP Infrastructure, Beta Tests, Use Cases, and Early Adopters

DHS		OMB	
NSA		IC	
OSD		DISA	
DOJ		EPA	
Army		NIST	
DOS			





SCAP Current State

- Current working with a beta version of SCAP
- Vendors self-assert SCAP capability
- The National Checklist Program and National Vulnerability Database are maintained as separate programs, with NVD hosting SCAP Content in flat file format
- IT products “read” SCAP Content from flat files
- Intermediate SCAP expertise required in operations personnel
- Federal sector is an early adopter of SCAP, but private sector understands SCAP value
- More use cases will emerge

SCAP Near-Term: SCAP in the Next Year

- SCAP Version 1.0 reaches full production
- The first "SCAP tools emerge from NVLAP testing in early calendar year 2008
- National Vulnerability Database becomes the Web interface to National Checklist Program content. NCP content is converted to SCAP format and imported into NVD.
- National Vulnerability Database enables import, export, and query capabilities for SCAP Content.
- IT products "read" SCAP Content through real-time, dynamic querying. Caching and/or flat file approaches are maintained for out-of-band circumstances only.
- Basic SCAP expertise is required in operations personnel
- Private sector beta testing and production implementation of SCAP technologies are increasing, partially attributable to PCI DSS v1.1. International organizations start to adopt SCAP with Spain and Japan likely early adopters.
- SCAP vulnerability management use cases are becoming fulfilled and/or are well integrated into technology roadmaps. Application of SCAP for compliance, configuration, and asset management is still subdued as all parties a) better understand how to apply SCAP technology in these domains and b) await fuller functionality of SCAP version 2.0.

SCAP Long-Term: SCAP in 2-5 Years

- SCAP Version 1.0 is in full production. SCAP Version 2.0 reaches full production.
- The SCAP tool conformance process is well-established and the list of SCAP products is large and inclusive of vulnerability, compliance, configuration, and asset management technologies
- SCAP is embedded and automated, requiring little knowledge of SCAP functionality from operations personnel.
- SCAP technologies are equally employed in Federal and private sectors. SCAP is used internationally.
- SCAP technologies reach beyond vulnerability management into compliance, configuration, change, asset, and other areas of IT management. The majority of initially envisioned use cases are fulfilled, but now new, more innovative SCAP use cases are emerging.

Presentation Summary

- A complex chain of events has increased security workload with little relief from automation
- SCAP sets the stage for automation and enables interoperability and repeatability as interim value
- SCAP partially automates compliance with FISMA and other security mandates
- All parties have some actions to bring the full value of SCAP to fruition
- Many product teams, service providers, and operations teams have already embarked on SCAP initiatives and are achieving results
- The value of SCAP will only grow over time as we evolve the protocol, the content, and our application of the technology

More Information

National Checklist Program — http://checklists.nist.gov

National Vulnerability Database — http://nvd.nist.gov or http://scap.nist.gov

- SCAP Checklists
- SCAP Capable Products
- SCAP Events

NIST FDCC Web Site — http://fdcc.nist.gov

- FDCC SCAP Checklists
- FDCC Settings
- Virtual Machine Images
- Group Policy Objects

NIST SCAP Mailing Lists — Scap-update@nist.gov

Scap-dev@nist.gov

Scap-content@nist.gov

Contact Information

100 Bureau Drive Mailstop 8930
Gaithersburg, MD USA 20899-8930

ISAP NIST Project Lead

Steve Quinn
(301) 975-6967
stephen.quinn@nist.gov

NVD Project Lead

Peter Mell
(301) 975-5572
mell@nist.gov

Senior Information Security Researchers and Technical Support

Karen Scarfone
(301) 975-8136
karen.scarfone@nist.gov

Murugiah Souppaya
(301) 975-4758
murugiah.souppaya@nist.gov

Matt Barrett
(301) 975-3390
matthew.barrett@nist.gov

Information and Feedback
Web: http://scap.nist.gov
Comments: scap-update@nist.gov

Questions

National Institute of Standards & Technology
Information Technology Laboratory
Computer Security Division